

NOKIA

DVB-CPT-710

Nokia

**Proposal for DVB
Content Protection & Copy Management
Technologies**

Version 1.0

NOKIA

Best Available Copy



Copyright © Nokia Inc. 2001. All rights reserved.

No part of this publication may be copied, distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language without the prior written permission of Nokia.

The manufacturer has made every effort to ensure that the instructions contained in the documents are adequate and free of errors and omissions. The manufacturer will, if necessary, explain issues which may not be covered by the documents. The manufacturer's liability for any errors in the documents is limited to the correction of errors and the aforementioned advisory services.

The documents have been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using them. The manufacturer welcomes customer comments as part of the process of continual development and improvement of the documentation in the best way possible from the user's viewpoint. Please submit your comments to the nearest Nokia sales representative.

NOKIA and the arrows logo are registered trademarks of Nokia Inc..

No. of Pages	Edited by/Translator	Author	Approved by	Previous issue (x) approved
87		15 Oct 2001 Jukka Alve, Peter Chiu, Zheng Yan	19 Oct 2001 JA	



Table of Contents

Summary of Revision.....	5
References	5
Acknowledgment	5
Abbreviations and Glossary	5
1 Contact Details	7
2 IPR Statement	8
3 Executive Summary	9
4 Architecture Description	11
4.1 Architectural Principles	11
4.2 Architectural Assumptions	11
4.3 Consumer Domain Model	11
4.4 Network Model	13
4.5 Conceptual Model	14
4.6 Content Flow Model	16
4.7 Trust Model	18
4.8 Payment Model	19
4.9 Usage State Record Concept	20
4.9.1 Usage State Record	20
4.9.2 Baseline Usage State Updating Rules	20
4.9.3 Usage State Extensions	21
4.9.4 Right Expression Language	21
4.10 Content Voucher Concept	23
4.10.1 Voucher Template	23
4.10.2 Content Voucher	24
4.10.3 Content Key Generation	25
4.11 Copy Protection Model	28
4.11.1 Content Copying Procedure	28
4.11.2 Content Key Encryption Scheme	29
4.11.3 Content Voucher Authentication	32
4.11.4 Threat Analysis	33
4.11.4.1 Illegal Content Copying	33
4.11.4.2 Illegal Content and Voucher Copying	34
4.11.4.3 Content Encryption Hacking	34
4.11.4.4 Usage State Tampering	35
4.12 Digital Watermarking Protection	36
4.13 Software Model	38
5 Proposed Functional Areas	39
5.1 CPCM System Preparations	39
5.1.1 Authorized Domain Registration	39
5.1.2 Authorized Domain Joining	41
5.1.3 Content Preparation and Distribution	43
5.1.3.1 CPCM-compliant Watermarking	43
5.1.3.2 Voucher Template Distribution Mechanisms	43
5.1.3.2.1 Voucher Template Delivery as CPCM-Specific Descriptor	43
5.1.3.2.2 Voucher Template Delivery via CPCM-Specific ECM/EMM	44
5.1.3.2.3 Voucher Template Delivery via CPCM-Specific PES	44
5.1.3.2.4 Voucher Template Delivery over IP Datacast	44
5.1.3.2.5 Voucher Template Delivery via Interactive Access Network	44
5.1.3.3 Voucher Template Protection during Distribution	44
5.2 CPCM-Compliant Operations	45



Contact Details

5.2.1	Content Recording	45
5.2.2	Content Downloading	47
5.2.3	Content Copying	48
5.2.3.1	Content Copying within Same Domain	48
5.2.3.2	Content Copying across Different Domains	49
5.2.3.3	Copy Control Not Asserted	51
5.2.4	Content Moving	53
5.2.4.1	Content Moving within Same Domain	53
5.2.4.2	Content Moving across Different Domains	53
5.2.5	Content Rendering	54
5.2.6	Content Backup and Restore	56
5.2.7	Content Superdistribution	57
5.2.8	Content Recording or Downloading First Pay Later	59
5.2.9	Content Uploading and Rendering in Mobile Devices	60
5.2.10	Content Streaming	61
5.2.11	Support of Multiple Domains per Device	62
5.3	Backward Compatibility	62
5.4	CPCM-compliant Content Entering Legacy System	62
5.5	Legacy Content Entering CPCM-compliant System	63
6	Protection Mechanism For Content	64
6.1	Proposed Algorithms and Functions	64
6.2	Content Encryption	64
6.3	Content Key Encryption	64
6.4	Voucher Integrity Protection	64
6.5	Tamper-Resistant Storage	64
6.6	Digital Watermarking	65
7	DVB CPCM API	66
7.1	Baseline CPCM API	66
7.1.1	Multiple Proprietary Extension Support	67
7.1.1.1	Installation and Authentication of Proprietary Extension Plug-ins	67
7.1.1.2	Identification of Proprietary Extension Plug-ins	68
7.1.2	Multiple Non-CPCM System Support	68
8	Underlying Security Infrastructure	71
9	Implementation Requirements	72
9.1	Object Sizes	72
9.2	Tamper-Resistant Storage	73
9.3	Non Tamper-Resistant Storage	73
9.4	CPCM Baseline Library	74
10	Usability	75
11	Renewability, Revocation and Resistance to Obsolescence	76
11.1	Renewability	76
11.1.1	System Software Upgrade	76
11.1.2	Domain Renewability	76
11.2	Revocation	76
11.2.1	Device Revocation	76
11.2.2	Domain Revocation	76
11.3	Resistance to Obsolescence	77
11.3.1	Scalability	77
11.3.2	Security Robustness	77
11.3.3	Foreseeable Circumvention Devices	77
12	Suitability for Import or Export	79
13	Current State of Development	80
14	Conformance Statement	81



Summary of Revision

#	Date	Author(s)	Comments
1.0	10.18.2001	Jukka Alve, Peter Chiu, Zheng Yan	Document created.

References

- [1] DVB Technical Module Ad-hoc Group on Copy Protection Technologies, "Call for proposals for copy protection technologies", revision 1.2, 7/5/2001
- [2] [HTTP://ODRL.NET](http://ODRL.NET)
- [3] ISO/TC46/SC9, "ISO Proposed Draft Technical Report 21449: Content Delivery and Rights Management: Functional Requirements for Identifiers and Descriptors for Use in the Music, Film, Video, Sound Recording and Publishing Industries", 6/13/2001
- [4] ISO/IEC 13818-1: Generic Coding of Moving Pictures and Associated Audio: (MPEG-2) Systems
- [5] TV-AnyTime web page about Content Reference ID, "<ftp://tva:tva@ftp.bbc.co.uk/./pub/Specifications/SP004v10.zip>"
- [6] ETSI TS 101 812 v1.1.1 (2000-07), "DVB Multimedia Home Platform Specification 1.0"

Acknowledgment

Other major contributors to this proposal include:

- Laurent Guillbez
- Parvez Ahammad
- Mauri Kangas.

Abbreviations and Glossary

This document follows the definition of abbreviations and glossary that are specified in [1]. All uncovered abbreviations are captured in the following table.

AES	Advanced Encryption Standard
CA	Conditional Access
CAT	Conditional Access Table
DRM	Digital Right Management



Contact Details

GSM	Global System for Mobile communications
ODRL	Open Digital Right Language
PES	Packetized Elementary Stream
PKI	Public Key Infrastructure
PMT	Programme Map Table
PSTN	Public Switch Telephone Network
SHA	Secured Hashing Algorithm
SSL	Secure Socket Layer
USB	Universal Serial Bus



1 CONTACT DETAILS

Primary contact name: Jukka Alve

Organization: Nokia

Telephone: +358 7180 36507

Fax: +358 7180 36214

Email: jukka.alve@nokia.com

Postal address: Nokia Venture Organization/Nokia Home Communications,
P.O.Box 407, FIN-00045 Nokia Group, Finland.

Backup contact name: Peter Chiu

Organization: Nokia

Telephone: 1-(781)-993-3917

Fax: 1-(781)-993-1914

Email: peter.k.chiu@nokia.com

Postal address: Nokia House, 5 Wayside Road, Burlington, MA, USA 01803.



2 IPR STATEMENT

Any intellectual property rights that Nokia has to the content of this proposal will adhere to the DVB IPR policy as formulated in the relevant sections in the DVB Memorandum of Understanding. To the extent that Nokia's contribution is adopted to any specification published by DVB, Nokia undertakes to license its Technically Necessary (Essential) patents on fair and reasonable, non-discriminatory terms and conditions complying with standardization obligations based on reciprocity.

3 EXECUTIVE SUMMARY

This proposal is in response to the DVB-CPT Call for Proposals for Content Protection and Copy Management Technologies. The objective of this proposal is to recommend a common framework that ensures authorized usage of content beyond the traditional boundary points of DVB CA systems. The common framework will provide answers to both premium content providers who want to protect their content from piracy, and free-to-air content providers who may also want to protect copyrights of their production. In this context, DVB distributed content covers conventional digital TV programmes and novel data broadcasting. The common framework also supports other content types such as pre-recorded media and Internet media, as well as new business models such as superdistribution. This proposal recommends a solution that possess the following benefits:

- The proposed solution is based on the concept of separate management of content and usage state in the form of voucher
- The proposed solution can be implemented using open standards and widely accepted cryptographic techniques, such as RSA, SHA, AES, SSL, PKI
- This proposed solution provides a secure and optimized method to manage content protection and copy management, which supports targeting content to an authorized device and/or authorized domain, based on conditional encryption of content encryption key depending on usage state
- The proposed solution provides the flexibility to support novel business models such as content superdistribution and "record/download first pay later", by managing usage state separated from content itself
- The proposed solution assumes the availability of an interactive access network, which facilitates the communication of authorized devices with service provider on an as-needed basis; always-on network connectivity is not required. The need of communication over the interactive access network is optimized, and only required during domain registration and deregistration, domain joining and leaving, voucher upgrade and renewal
- The proposed solution complements rather than competes with other DRM or CA based solutions to furnish an end-to-end CPCM solution; DRM and CA based solutions can choose to terminate their services at the border of the adjoined CPCM system, and content is repackaged into CPCM-compliant format
- The proposed solution addresses backward compatibility with millions of existing DVB consumer electronics equipment, by minimizing the requirement at the broadcast sources, and only effecting the CPCM control after content terminates its native protection service (e.g. CA, DRM) at the boundary of CPCM and broadcast domain
- The proposed solution applies digital watermark technology to positively identify a piece of content as CPCM-protected, i.e. to distinguish it from



Executive Summary

legacy content. The watermark also provides a tamper-resistant method to associate the content with the corresponding untargeted voucher delivered in the broadcast bitstream.

4 ARCHITECTURE DESCRIPTION

This chapter establishes the DVB CPCM architecture by analyzing the commercial requirements using different architectural models.

4.1 Architectural Principles

To comply with [1], the proposed architecture adheres to the following principles as much as possible:

- Openness
- Interoperability
- Flexibility
- Market driven.

4.2 Architectural Assumptions

The proposed architecture makes the following assumptions:

- It is assumed that content protection service discontinuity at the boundary of broadcast and CPCM domains can be implemented seamlessly, such that piracy attack at device level will not be possible
- It is assumed that tamper-resistant storage is available in CPCM-compliant devices for secured storage of confidential information, such as device private key and domain symmetric key
- All analog devices are considered as legacy devices from the DVB CPCM perspective, and treated accordingly by the proposed CPCM system
- It is assumed that CPCM-compliant devices are implemented in such a way that they protect against piracy attacks of any content that needs to be temporarily buffered in device memory in clear form during processing. Exception is content with usage state "Copy control not asserted and domain traversal allowed", in which case no content encryption is necessary.

4.3 Consumer Domain Model

Figure 1 illustrates the consumer domain model [1], which represents the in-home digital network environment where various types of consumer electronics devices are connecting together to share DVB and other digital media delivered through broadcast network, the Internet, and pre-recorded media like DVD. The model introduces the concept of authorized domain.

An authorized domain is defined as an assembly of DVB consuming authorized devices, networks, and interfaces, which are used primarily by an authorized

user both inside and outside of the home and owned/rented by that user. Logically speaking, an authorized domain represents the association between usage rights of DVB content and the group of authorized devices owned by a person. This association can be extended to the group of authorized devices owned by a group of people, e.g. a family, who are willing to or finding it convenient to share the usage rights of DVB content among themselves and thus registered as a single authorized domain.

In this context, an authorized device is one that has acquired the rights to consume a piece of DVB content. Typical ways to acquire a usage right include DTV subscription and pay-per-view.

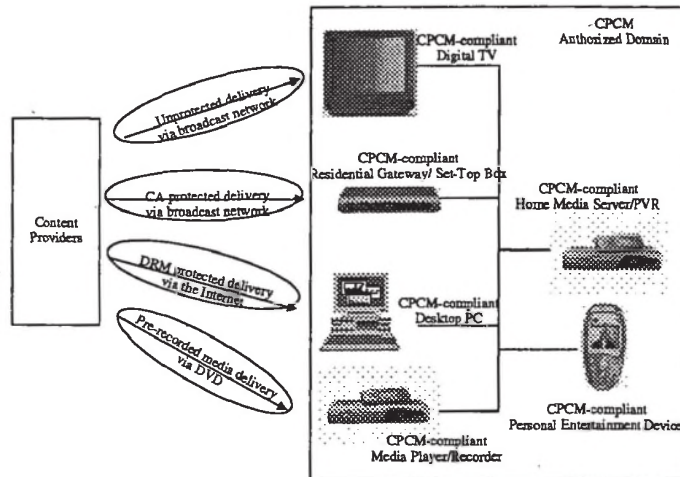


Figure 1: Consumer Domain Model

4.4 Network Model

Figure 2 illustrates the DVB CPCM network model.

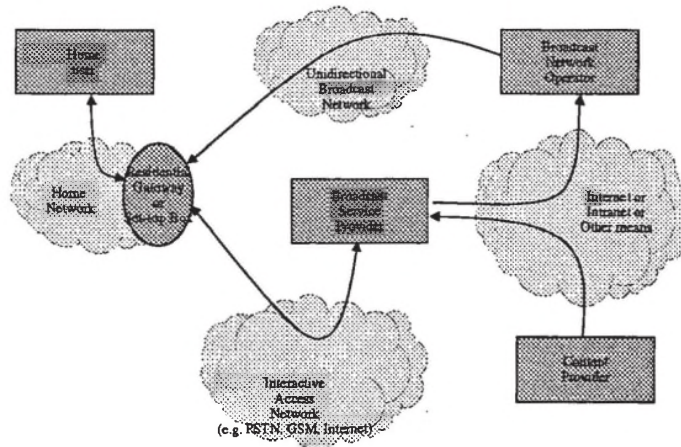


Figure 2: Network Model

Content provider can offer their contents to home users via broadcast service provider or the Internet. Broadcast service provider converts the DVB contents into CPCM-compliant format, and deliver them over the unidirectional broadcast networks managed by broadcast network operator. Broadcast service provider also makes use of an interactive access network (e.g. PSTN, GSM, the Internet) to communicate content ordering information with home users. Home users receive digital contents from DVB network, the Internet and pre-recorded media, as well as interact with broadcast service provider via a residential gateway or set-top box.

4.5 Conceptual Model

Figure 3 illustrates the DVB CPCM conceptual model.

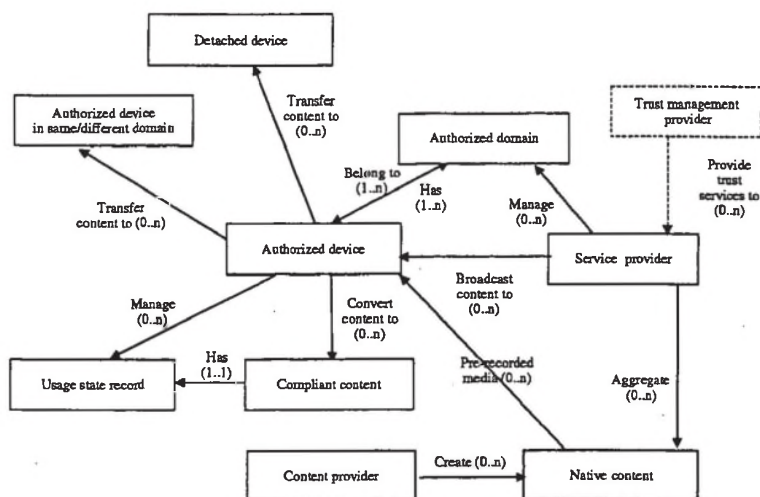


Figure 3: Conceptual Model

Content provider creates content in native format. Service provider aggregates these native contents, and prepares them ready for broadcast. The content received by an authorized device may be in the form of CA-protected broadcast, free-to-air broadcast, DRM-protected datacast, or pre-recorded media. Service provider supports the DVB CPCM architecture by the formation of authorized domains, via domain registration and domain joining.

An authorized domain consists of one or more authorized devices. On the other hand, an authorized device may belong to more than one authorized domain. Authorized devices within the same authorized domain can share content usage freely as long as the usage state allows. If content is transferred across domain boundary for consumption, authorized device needs to contact service provider to obtain additional usage right, unless cross-domain transfer is allowed.

When a piece of content enters an authorized domain the first time, its native protection service (e.g. clear-format, CA or DRM) will be terminated, and the CPCM protection service will be applied to the content. That means the content is converted into CPCM-compliant format, and associated with a usage state record. Authorized devices make use of usage state record to manage consumption of CPCM-compliant content.

CPCM-compliant content can also be transferred to detached devices. Detached devices are defined as those devices that do not possess any CPCM functionality (e.g. backup storage device), and not registered with any service provider.

The trust management provider concept is introduced to the CPCM architecture to solve the following problems:

- Authorized devices within the same authorized domain may be built by different equipment vendors. Equipment vendors may build their devices based on different trust infrastructures (e.g. Certificate authority). How can the diverse trust infrastructures be aligned?
- Consumers may obtain their broadcast services from different service providers. If a consumer wants to share a piece of content with another consumer registered with a different service provider, how can the transaction of usage right transfer be executed?
- Novel business models such as content superdistribution require a trusted third party to facilitate financial and usage clearing among content providers, service providers and consumers.

A trust management provider offers trust services to multiple service providers to handle the aforementioned issues. However, this is a new business model, and may take time to establish itself. Hence the trust management provider concept is considered optional in this proposal, and some of the trust management provider functionality may be supported by individual service providers themselves.

4.6 Content Flow Model

Figure 4 illustrates the DVB CPCM content flow model. As shown in the figure, allowed content sources for a CPCM system include:

- Clear or CA-scrambled content from broadcasting sources like DVB-T, DVB-C, DVB-S
- Clear or encrypted content from pre-recorded media sources
- Clear or DRM-encrypted content from the Internet
- Clear or DRM-encrypted content from the Internet via detects

Note that in the special case of CA-based broadcasting and backward compatibility is not an issue, content may be encrypted in CPCM-compliant format by content or service provider before CA-scrambling is applied on it.

Within a CPCM system, the following content flows are allowed:

- CPCM-encrypted content transferred within an authorized domain
- CPCM-encrypted content transferred from one authorized domain to another authorized domain
- CPCM-encrypted content transferred to a detached authorized device
- CPCM-encrypted content transferred to a detached device.

The content flow within a CPCM system is enabled by typical transport mechanisms such as FTP, IEEE1394, USB, DVD, ... etc.

Authorized devices can be categorized into the following categories:

- Border devices that act as a gateway between the in-home network and the broadcast network or the Internet. Border devices terminate native content protection services such as CA or DRM, and transfer to CPCM control. A typical example of border device is set-top box
- Non-border devices that function purely within the CPCM environment, and do not receive content directly from broadcast network. A typical example of non-border device is personal video recorder without a CA module
- Detached authorized devices that have registered with the CPCM system, but lose connectivity to the interactive network access either permanently or temporarily, such that they cannot obtain CPCM services from service provider. The functionality of this type of device is limited to content consumption and storage.

Note that backup storage is considered as detached device, and it does not have any CPCM functionality, and is not considered as an authorized device.

In addition, authorized domain is a logical concept, and devices belonging to the same authorized domain are not necessarily collocated physically and connected by a LAN. An authorized device can connect to other devices within the same authorized domain via remote access technology (e.g. Dial-up modem).

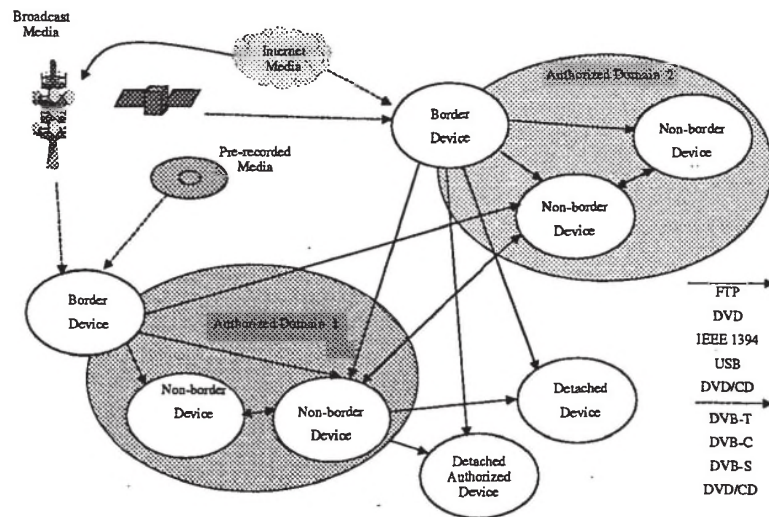


Figure 4: Content Flow Model

4.7 Trust Model

Figure 5 illustrates the trust model that must be established by the DVB CPCM system before content and usage right can be transferred safely between two entities in the system.

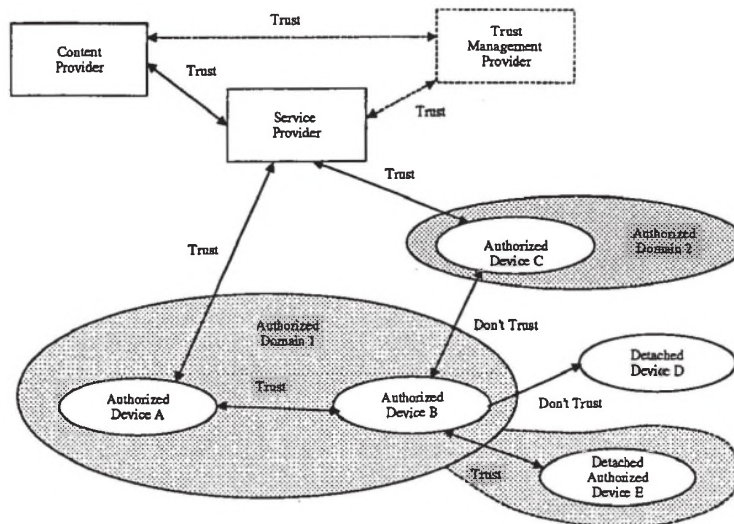


Figure 5: Trust Model

The trust between content provider and service provider (and optionally trust management provider) is defined by business agreement.

Service provider establishes trust with authorized domain and authorized device during domain registration and domain joining.

Within the same domain, authorized devices trust each other. Content and usage rights are transferred between the devices on a peer-to-peer basis, without the intervention of service provider. The only exceptions are usage right upgrade or renewal. This applies to detached authorized device, which is temporarily isolated from an authorized domain.

Across authorized domains, authorized devices do not trust each other, and require the intervention of service provider to assist in transfer of usage right.

No trust can be established between authorized device and detached device.

On the other hand, the trust model is dependent on the nature of the content itself. For example, if the content is free-to-air without any requirement of copyright protection from content provider, the trust boundary between authorized domains will disappear.

4.8 Payment Model

Figure 6 illustrates the DVB CPCM payment model.

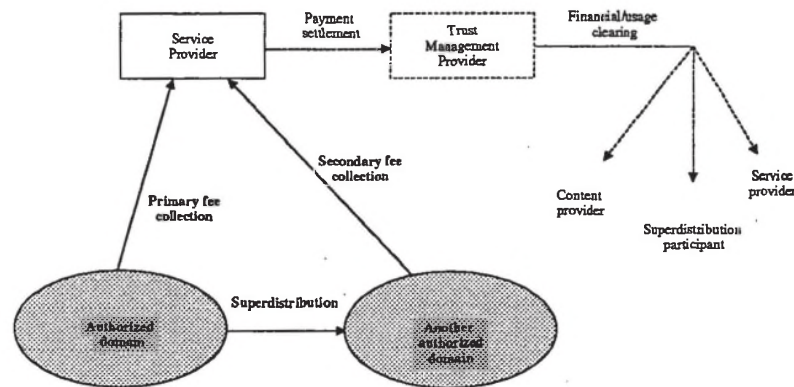


Figure 6: Payment Model

An authorized domain acquires usage rights via conventional channels. For example, a DTV subscriber pays monthly subscription and pay-per-view fees to broadcast service provider, and an online shopper pays for a piece of digital content via credit card over the Internet. These payments are categorized as primary fee collections.

When a piece of CPCM-compliant content is transferred from the owner authorized domain to another authorized domain, the usage rules associated with the content may mandate that the receiving domain pays for the usage rights as well. This type of transactions is called superdistribution, and the associated payments are categorized as secondary fee collection.

The CPCM superdistribution model suggests that service provider collects the secondary fees on behalf of the other beneficiaries. The payment settlement is then collected by trust management provider, which subsequently clears the financial and usage transactions. The beneficiaries of the superdistribution transactions will be credited accordingly.

Since content superdistribution is a novel business model, and requires substantial business alignment among content providers and service providers, the CPCM architecture considers this an optional functionality during initial implementation.

4.9 Usage State Record Concept

The concept of usage state record is introduced to support content protection and copy management, by offering a data structure that stores the content usage state along with associated control flags.

4.9.1 Usage State Record

The CPCM usage state record has the following data structure:

Table 1: Usage State Record

Field Name	Minimum Size	Optional Values	Default Value
Usage State Baseline	2 bits	<ul style="list-style-type: none"> Copy control not asserted Copy once Copy no more Copy never 	Copy control not asserted
Usage State Extension	4 bits	TBD	N/A
Domain Traversal Flag	1 bit	<ul style="list-style-type: none"> Allowed Disallowed 	Allowed
Usage State Change Flag	1 bit	<ul style="list-style-type: none"> Allowed Disallowed 	Allowed
Total size of data structure = 8 bits			

Remarks:

- (1) The domain traversal flag is used to indicate that a piece of content is allowed or disallowed to be transferred across authorized domains
- (2) The usage state change flag can be used to indicate that a piece of content is allowed or disallowed to have its usage state modified during its lifecycle in a CPCM system.

4.9.2 Baseline Usage State Updating Rules

Some general usage state updating rules are:

Table 2: Baseline Usage State Updating Rules

Item	Original Usage State	Condition	New Usage State
------	----------------------	-----------	-----------------

1	Not available	Legacy content entering CPCM system	Copy control not asserted, domain traversal allowed, usage state change allowed
2	Unrecognizable or corrupted usage state	Content entering CPCM system	Copy never, domain traversal disallowed, usage state change disallowed
3	Copy control not asserted	Content copying	Copy control not asserted
4	Copy once	Content copying	Copy no more
5	Copy no more	Content copying	N/A
6	Copy never	Content copying	N/A
7	Some usage state	Content moving	Same usage state
8	Some usage state	Usage state renewal	Same usage state
9	Copy no more	Usage state upgrade	Copy once

4.9.3 Usage State Extensions

Usage state extensions may be applied to CPCM-compliant system as proprietary extension plug-ins. Every usage state extension must define a mapping to a baseline usage state for interoperability consideration.

4.9.4 Right Expression Language

It is proposed that DVB CPT consider to expand the current baseline usage state model to a more comprehensive model based on right expression language technology (e.g. ODRL). Right expression language technology provides efficient and effective way to support rich and flexible business models, and renders usage state extension and proprietary plug-ins unnecessary. The following table shows some examples of how the DVB CPCM baseline usage states can be implemented using ODRL [2]:

Table 3: ODRL Implementation of DVB CPCM Usage State

DVB CPCM Usage State Record			ODRL Example
Usage State	Domain Traversal	Usage State Change	

Copy control not asserted	Allowed	Disallowed	<pre> <rights> <usage> <asset><uid>abc</uid></asset> <copy></copy> </usage> </rights> </pre>
Copy once	Allowed	Disallowed	<pre> <rights> <usage> <asset><uid>abc</uid></asset> <copy><constraint><count>1</count> </constraint></copy> </usage> </rights> </pre>
Copy no more	Allowed	Disallowed	<pre> <rights> <usage> <asset><uid>abc</uid></asset> </usage> </rights> </pre>
Copy never	Allowed	Disallowed	<pre> <rights> <usage> <asset><uid>abc</uid></asset> </usage> </rights> </pre>

ODRL supports the concept of "group" constraint, which can be used to implement the domain traversal concept in DVB CPCM baseline model. An example is:

```

<group>
  <context>
    <uid>any-domain</uid>
  </context>
</group>

```

4.10 Content Voucher Concept

The concept of content voucher is introduced to support content protection and copy management, by offering a logical binding of content with its usage right.

Content vouchers are instances of their corresponding voucher template. A voucher template is a content-specific data structure that can be instantiated into a content voucher by adding the device-targeted information such as content encryption key and device digital signature.

4.10.1 Voucher Template

Content Voucher template is defined as the following data structure:

Table 4: Content Voucher Template

Field Name	Size	Remarks
CPCM Version Number	16 bits	To support CPCM version control
CPCM Proprietary Extension Number	16 bits	To support CPCM proprietary extension identification
Voucher ID	64 bits	Blank for voucher template For voucher, generated by border device, as a function of domain ID, device ID and content ID
Content ID	64 bits	Standard-based content ID, e.g. ISO/MPEG
Service Provider ID	32 bits	To support multiple domain registration of authorized device
Initial Domain ID	32 bits	This field will store the initial domain ID right after the voucher template is converted into a content voucher
Current Domain ID	32 bits	Current domain ID of voucher holding device Blank field in voucher template
Usage State Record	8 bits	Service provider assigned usage states Usage state extension has been considered

Content Key Status	2 bits	Options: 00 = no content key, no seed, generate content key locally using random number generator 01 = no content key, no seed, get key from service provider 10 = voucher contains seed, generate content key by content ID and shared secret 11 = voucher contains content key
Content Key (or content key seed)	128 bits	Symmetric encryption key (128-bit block) in content voucher This field may contain content key seed, depending on the content key status field, in voucher template
Digital Signature	160 bits	Using SHA-1 as hashing function Digitally signed by service provider private key or device private key
Total size of data structure = 554 bits		

The content ID is a globally unique identification. The content ID should be created and managed by content provider. It is recommended that content ID assignment follow standards such as ISO [3,4,5].

Voucher template may be created by service provider. It is delivered to authorized domains via broadcast bitstream. The data integrity of voucher template is protected by digital signature of service provider. It is also envisaged that voucher template can be targeted to single or multiple authorized devices for special contents, e.g. pay-per-view. Voucher template may be broadcasted periodically during the entire period of content broadcast.

4.10.2 Content Voucher

A content voucher is generated by a CPCM-compliant border device and logically bound to a piece of content when the content first enters a CPCM system. A content voucher is created by instantiating the corresponding voucher template. The content voucher remains associated with the content logically for the entire lifecycle of the content. A content voucher has the same data structure as voucher template.

4.10.3 Content Key Generation

Content key is a symmetric encryption key. It is used to encrypt a piece of content when it first enters a CPCM system. Content key can be generated and/or distributed using one of the following methods:

Table 5: Content Key Generation Methods

Method	Advantages	Disadvantages
Local random key generation by border device	<ul style="list-style-type: none"> Breaching of one content key will not affect others 	<ul style="list-style-type: none"> Content or service provider does not know how to regenerate the voucher that contains content key if destroyed
Local key generation by border device, based on content ID and shared secret with service provider	<ul style="list-style-type: none"> Content or service provider can regenerate content key based on shared secret information 	<ul style="list-style-type: none"> It requires extra effort to identify shared secret (e.g. original domain ID must be transferred along with content so that the corresponding secret domain symmetric key can be identified by service provider during content key regeneration)
Content key generated and supplied by service provider via interactive network access	<ul style="list-style-type: none"> Content or service provider can re-supply content key if necessary 	<ul style="list-style-type: none"> Network access delay may affect CPCM system performance seriously Service provider may receive large amount of simultaneous requests
Content key generated and supplied by service provider via voucher template delivery, e.g. CPCM-specific ECM/EMM	<ul style="list-style-type: none"> Content or service provider can re-supply content key if necessary 	<ul style="list-style-type: none"> Voucher template may be tampered by hacker

Each of the aforementioned methods of content key generation has its pros and cons. It is recommended that the CPCM system offer flexibility in implementing the content key generation. The selected content key generation method is indicated by the 2-bit data field called "content key status" in the voucher template data structure. Depending on the content key status, the content key data field in the voucher template data structure may contain the content key generated by service provider, or the content key seed for local key generation. The options are:

- Local key generation based on shared secret

This method is applicable for content that service provider has not applied CPCM-compliant encryption at broadcast source, and service provider is willing to offer voucher upgrade and renewal services upon request.

- Local random key generation

This method is applicable for content that service provider does not expect to offer voucher upgrade or renewal service, e.g. free-to-air content with usage state "Copy control not asserted and domain traversal disallowed", in which case the content will still be encrypted, based on the copy protection model

- Service provider supplied content key via Interactive network delivery

This method is applicable for special content, e.g. pay-per-view movies, that service provider will have interaction with consumers anyway.

- Service provider supplied content key via CPCM-specific ECM/EMM

This method is applicable for high-value content that service provider has already generated content key by itself and ready to re-issue voucher upon request.

For reference purpose, an example of the local key generation based on shared secret is described below:

- Service provider does not apply any CPCM-compliant encryption to the content at broadcast source, but sets the content key generation method to "Local key generation based on shared secret", and plants a content key seed in the voucher template. This content key seed is a function of content ID and is remembered by service provider
- When a border device receives the voucher template, it understands from the content key generation method field that it needs to generate a content key locally using the content key seed
- The border device then generates the content key as a function of the content key seed and the domain symmetric key of the border device
- The domain ID of this border device, called "initial domain ID", is remembered in the content voucher, and this piece of information can be backed up by subsequent devices separate from the voucher if necessary
- If the voucher is lost in subsequent content transfer, the authorized device in trouble can contact service provider for voucher renewal, by supplying the service provider with the information including content ID, original domain ID. The service provider can regenerate the content key, because it knows the domain symmetric key related to the original domain ID, and the content key seed related to the content ID
- Hackers cannot break this key generation method, because the domain symmetric key is a shared secret between service provider and authorized device, and this key is kept in device tamper-resistant storage that is only accessible by CPCM-enabled kernel.



Architecture Description

In the remaining chapters of this document, the method of local key generation algorithm based on shared secret is assumed in the analysis.

4.11 Copy Protection Model

Figure 7 illustrates the copy protection model that can be used to describe the copy protection procedures offered by the CPCM architecture.

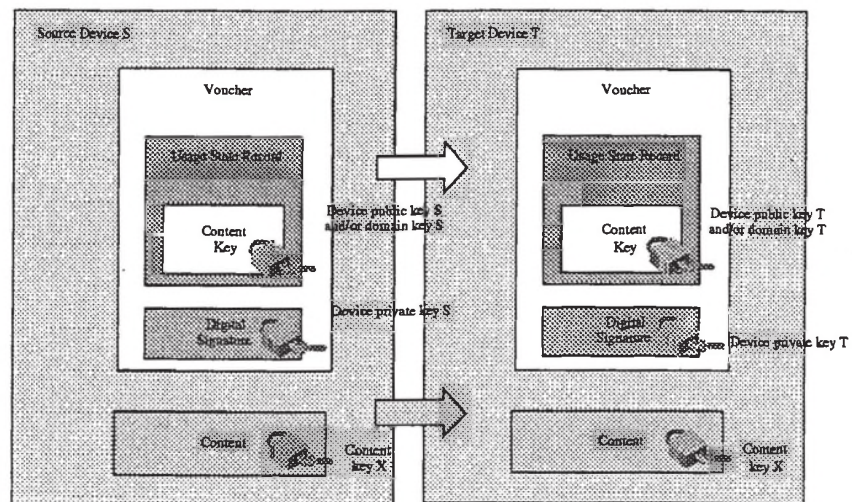


Figure 7: Copy Protection Model

4.11.1 Content Copying Procedure

This section illustrates the typical procedure that a piece of CPCM-compliant content is transferred from a source device S to a target device T in different domain. Both the content and the associated voucher are copied (or moved) during the operation. It is assumed that the content is allowed to be copied across authorized domains. Note that the procedure will be similar in the case of content copying within the same domain.

Table 6: Content Cross-Domain Copying Procedure

Stage	Description
Pre-conditions	<ul style="list-style-type: none"> Content is encrypted using a content key Content key is encrypted using source device public key and/or source device domain (symmetric) key Data integrity of content voucher is protected by digital signature of

	<p>source device</p> <ul style="list-style-type: none"> Content usage state record specifies that the content is allowed to be transferred across authorized domains
Procedures	<ol style="list-style-type: none"> A secured communication channel is established between the source device and target device, after mutual authentication (e.g. using SSL) Target device supplies its own domain ID and device public key, and the desired content ID to source device; source device supplies its own device public key to target device Source device determines that target device belongs to a different domain, and the desired content is allowed to be copied across authorized domain Source device updates its own copy of the content voucher, by updating the usage state, regenerate the digital signature using its own device private key. Source device generates a new copy of content voucher to be sent to target device, by first decrypting the content key with its own device private key and/or domain key, and then encrypting the content key using the target device public key, and finally generating the digital signature using its own device private key Target device verifies the authenticity and integrity of the incoming content voucher using the source device public key to decrypt the digital signature Target device regenerates the digital signature for the content voucher using its own device private key to protect the integrity and restore the consistency of the content voucher
Post-conditions	<ul style="list-style-type: none"> Content is encrypted using the same content key Content key is encrypted using target device public key and/or target device domain (symmetric) key Data integrity of content voucher is protected by digital signature of target device

4.11.2 Content Key Encryption Scheme

The proposed CPCM architecture recognizes that, depending on the original usage state of the content and the operation to be performed, there may be different requirements for content key encryption. For example, content with a usage state of "Copy Control Not Asserted" and domain traversal flag of "Allowed" does not need any protection of the content key; actually in this case, there is no requirement to protect the content by encryption at all. Hence a unique content key encryption scheme is recommended to offer optimized



Architecture Description

protection of content key, by conditionally encrypting content key using device public key and/or domain symmetric key.

The following state tables summarize the requirement of content key encryption under different state transitions. Note that the order of encryption (i.e. device public key first domain symmetric key second or vice versa) is not important as long as it is consistent.

Table 7: State Transition Within Authorized Domain

Original Usage State [Encryption Key Applied]	Domain Traversal Flag	Usage State after operation within same Authorized Domain [Encryption Key Required]			
		Move		Copy	
		Source File	Target File	Source File	Target File
Copy Control Not asserted	Allowed	Content and voucher erased	Copy Control No Asserted	Copy Control Not Asserted	Copy Control Not Asserted
Copy Once [Device Public Key S]	Allowed	Content and voucher erased	Copy Once [Device Public Key T]	Copy No More [Device Public Key S]	Copy No More [Device Public Key T]
Copy No More [Device Public Key S]	Allowed	Content and voucher erased	Copy No More [Device Public Key T]	Illegal operation	Illegal operation
Copy Never [Device Public Key S]	Allowed	Content and voucher erased	Copy Never [Device Public Key T]	Illegal operation	Illegal operation
Copy Control Not Asserted [Domain Symmetric Key S]	Disallowed	Content and voucher erased	Copy Control Not Asserted [Domain Symmetric Key S]	Copy Control Not Asserted [Domain Symmetric Key S]	Copy Control Not Asserted [Domain Symmetric Key S]
Copy Once [Domain Symmetric Key S] [Device Public Key S]	Disallowed	Content and voucher erased	Copy Once [Domain Symmetric Key S] [Device Public Key T]	Copy No More [Domain Symmetric Key S] [Device Public Key S]	Copy No More [Domain Symmetric Key S] [Device Public Key T]
Copy No More [Domain Symmetric Key S] [Device Public Key S]	Disallowed	Content and voucher erased	Copy No More [Domain Symmetric Key S] [Device Public Key T]	Illegal operation	Illegal operation
Copy Never [Domain Symmetric Key S] [Device Public Key S]	Disallowed	Content and voucher erased	Copy Never [Domain Symmetric Key S] [Device Public Key T]	Illegal operation	Illegal operation



Architecture Description

Table 8: State Transition Across Authorized Domains

Original Usage State [Encryption Key Applied]	Domain Traversal Flag	State after operation across Authorized Domains [Encryption Key Required]			
		Move		Copy	
		Source File	Target File	Source File	Target File
Copy Control Not asserted	Allowed	Content and voucher erased	Copy Control Not Asserted	Copy Control Not Asserted	Copy Control Not Asserted
Copy Once [Device Public Key S]	Allowed	Content and voucher erased	Copy Once [Device Public Key T]	Copy No More [Device Public Key S]	Copy No More [Device Public Key T]
Copy No More [Device Public Key S]	Allowed	Content and voucher erased	Copy No More [Device Public Key T]	Illegal operation	Illegal operation
Copy Never [Device Public Key S]	Allowed	Content and voucher erased	Copy Never [Device Public Key T]	Illegal operation	Illegal operation
Copy Control Not Asserted [Domain Symmetric Key S]	Disallowed	Illegal operation	Illegal operation	Illegal operation	Illegal operation
Copy Once [Domain Symmetric Key S] [Device Public Key S]	Disallowed	Illegal operation	Illegal operation	Illegal operation	Illegal operation
Copy No More [Domain Symmetric Key S] [Device Public Key S]	Disallowed	Illegal operation	Illegal operation	Illegal operation	Illegal operation
Copy Never [Domain Symmetric Key S] [Device Public Key S]	Disallowed	Illegal operation	Illegal operation	Illegal operation	Illegal operation

4.11.3 Content Voucher Authentication

Figure 8 illustrates how voucher authentication works in this copy protection model.

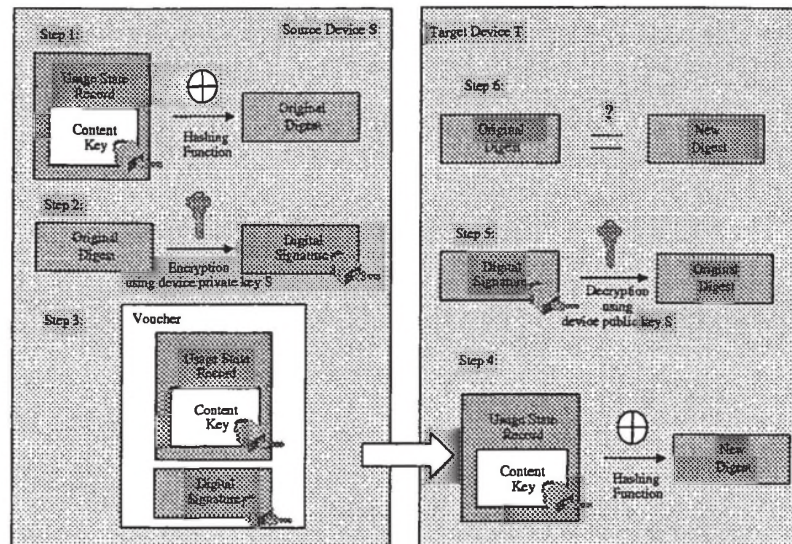


Figure 8: Voucher Authentication

The operational procedure of voucher authentication is described in the following steps:

1. At the source device, the raw voucher content, including usage state record and encrypted content key, is passed through a hashing function to produce an original message digest
2. A digital signature is generated when the original message digest is encrypted using the private key of the source device
3. The raw voucher content is packed with the digital signature into a content voucher, which is sent to the target device
4. The target device takes the raw voucher content and generates a new message digest based on the same hashing function as in the source device
5. The target device then uses the source device public key to decrypt the digital signature to obtain the original message digest

6. Finally, the original message digest is compared with the new one to determine if the voucher is intact and actually signed by source device before.

4.11.4 Threat Analysis

The following sections describe how the copy protection model counters illegal operations on CPCM-compliant content.

4.11.4.1 Illegal Content Copying

Figure 9 illustrates the scenario that only the encrypted content is illegally copied from the filesystem of a CPCM-compliant source device.

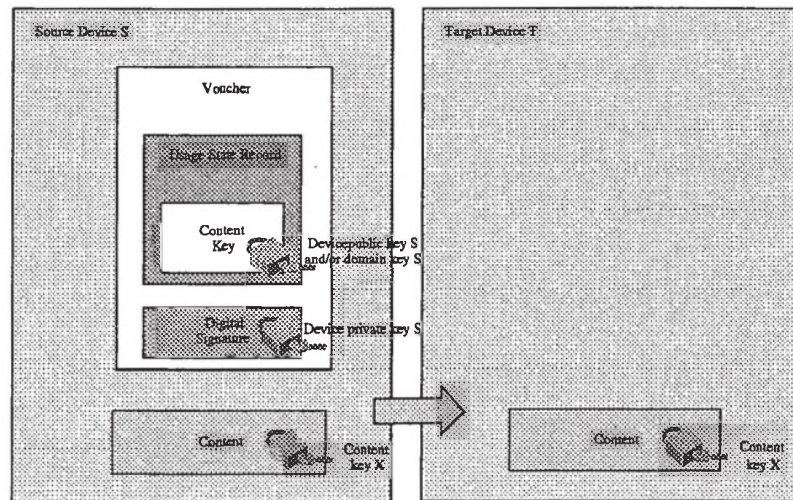


Figure 9: Illegal Content Copying

The target device cannot consume the content because the content is encrypted by an unknown content key. If the target device is CPCM-compliant, it cannot find the associated voucher, and needs to contact service provider to solicit a new voucher based on the content ID.

4.11.4.2 Illegal Content and Voucher Copying

Figure 10 illustrates the scenario that both the content and voucher are illegally copied from the filesystem of a CPCM-compliant source device.

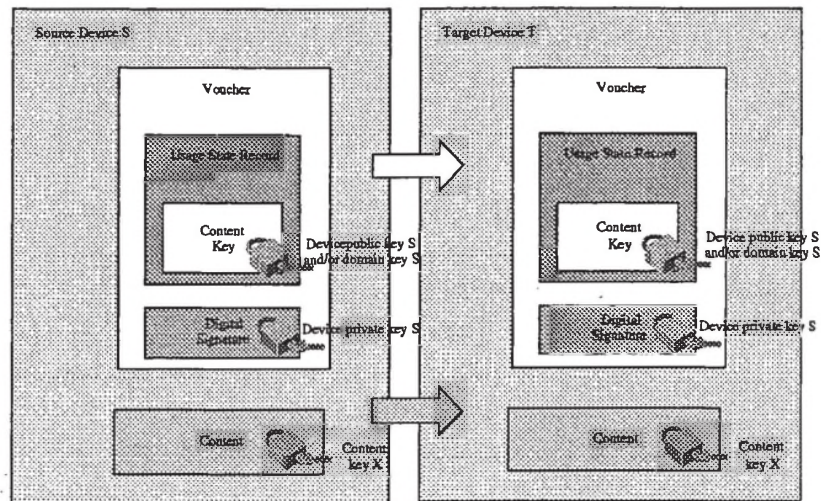


Figure 10: Illegal Content and Voucher Copying

The target device cannot extract the content key from the voucher because it does not possess the device private key of source device. If the target device is CPCM-compliant, it also fails to verify the integrity of the voucher because it may not have the public key of the source device. It can contact service provider to solicit a new voucher based on the content ID.

4.11.4.3 Content Encryption Hacking

A malicious user may attempt to hack a piece of content that was legally obtained via CPCM system. The bad intention is to obtain the content key in clear form, which can be used to decrypt the encrypted content.

However the CPCM architecture mandates that the device private key and domain symmetric key be stored in tamper-resistant storage, and its access is restricted to trusted CPCM kernel. Hence the hacker cannot access the device private key and/or domain symmetric key, and thus cannot decrypt the encrypted content.

4.11.4.4 Usage State Tampering

There are at least the following scenarios to consider in case of usage state tampering:

- Since content voucher transferred from source device to target device is protected by secured and authenticated communication channel, it is not likely that usage state in content voucher be tampered during transit
- If a malicious user performs illegal copy of both content and associated voucher from source device to target device, the malicious user can modify the usage state in the content voucher, and generate a totally new digital signature if he/she knows the hashing algorithm and has access of the target device private key. However, the malicious user does not have the source device private key to decrypt the content key, and thus the usage state tampering is fruitless
- If a malicious user performs a legal copy of both content and associated voucher from source device to target device, the malicious user may attempt to modify the usage state in the content voucher to gain extra usage right illegally. The malicious user can modify the usage state, but he/she cannot generate a proper digital signature by itself because target device private key is stored in tamper-resistant storage, and its access is restricted to trusted CPCM kernel.

4.12 Digital Watermarking Protection

The proposed CPCM architecture recommends to apply imperceptible digital watermark (e.g. invisible watermark for digital video, non-audible watermark for digital audio) to a piece of content. The advantages of the digital watermark include:

- Provide tamper-resistant proof of copyright ownership
- Support CPCM version control
- Provide positively identify that content is CPCM-compliant (not legacy content)
- Provide a backward-compatible, tampering-resistant mechanism to support content voucher template distribution

The digital watermark consists of the following payload structure:

Table 9: Digital Watermark Payload Structure

Attribute Name	Size	Remarks
Compressed Content ID	32 bits	Compressed by standard digital techniques such as hashing, message authentication code
Compressed Content/Service Provider ID	16 bits	Compressed by standard digital techniques such as hashing, message authentication code
CPCM Version Number	16 bits	To support CPCM version control
Total size of data structure = 64 bits		

There are many proprietary digital watermarking technologies in the industry, and Figure 11 illustrates one of the general approaches to apply and recover digital watermark.

Watermark application may be performed by content provider before supplying to service provider. The public watermark key is also sent to service provider, who will distribute to authorized devices during domain registration and joining. Authorized device must equip with a watermark recovery module to detect the presence of the CPCM-compliant watermark.

However, digital watermarking technology is still in the developing phase and there is no standard algorithm in the industry. It will probably take some time

before an acceptable watermarking detector can be implemented in devices. In the meantime, the copyright descriptor as specified in ISO 13818-1 may be used to provide the association between content and voucher template, even though this method is not tamper-proof as digital watermarking.

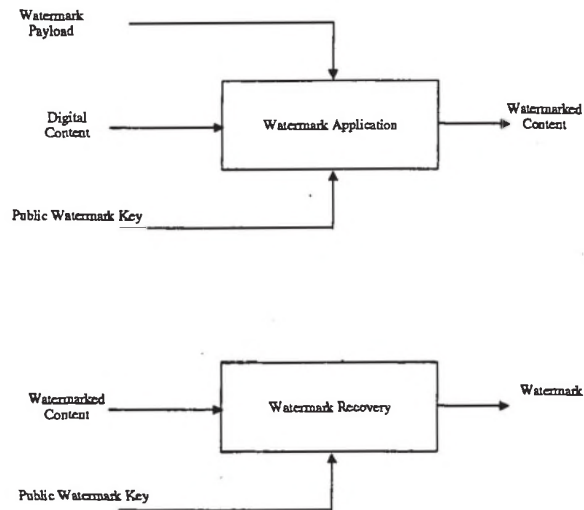


Figure 11: Digital Watermark Application and Recovery

4.13 Software Model

Figure 12 illustrates the software model of a DVB CPCM system that supports multiple proprietary CPCM plug-ins.

As stated in [1], proprietary CPCM extension systems are likely to exceed the CPCM baseline system, and hence the underlying business model supported. For example, different content providers may use different sets of usage state extension to specify additional business rules for authorized usage of CPCM-protected content. The CPCM software model consists of a baseline CPCM system, in which applications are supported by the baseline CPCM manager and library. Proprietary software plug-ins can be introduced to support proprietary CPCM extensions. This proprietary plug-ins make use of the baseline library via baseline APIs.

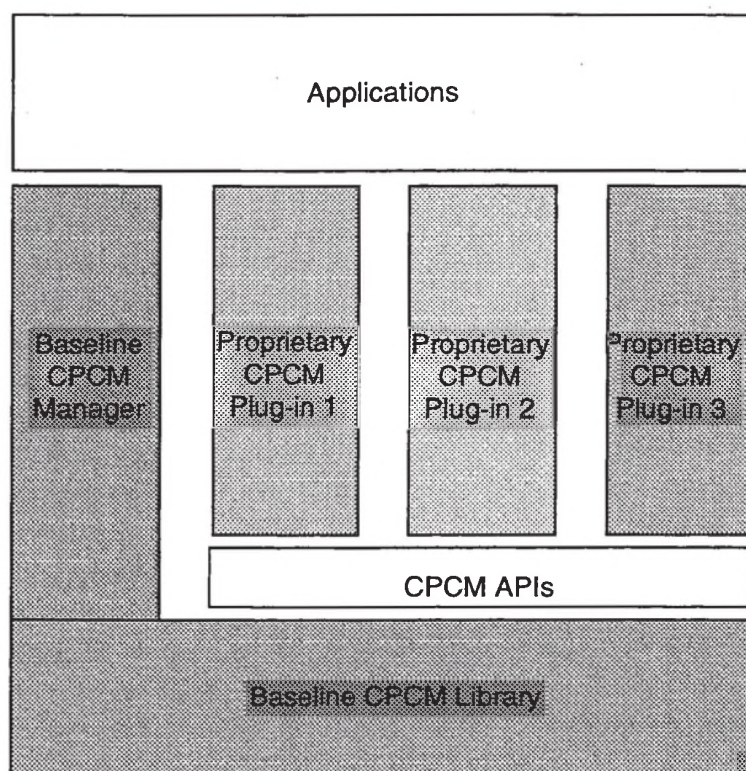


Figure 12: Software Model

5 PROPOSED FUNCTIONAL AREAS

This chapter describes the major functional areas addressed by the proposed DVB CPCM architecture. The functionality can be categorized into the following groups:

- CPCM system preparations
- CPCM-compliant operations
- Backward compatibility

5.1 CPCM System Preparations

5.1.1 Authorized Domain Registration

Figure 13 illustrates the typical procedure for a border device of an authorized domain to register with the DVB CPCM system.

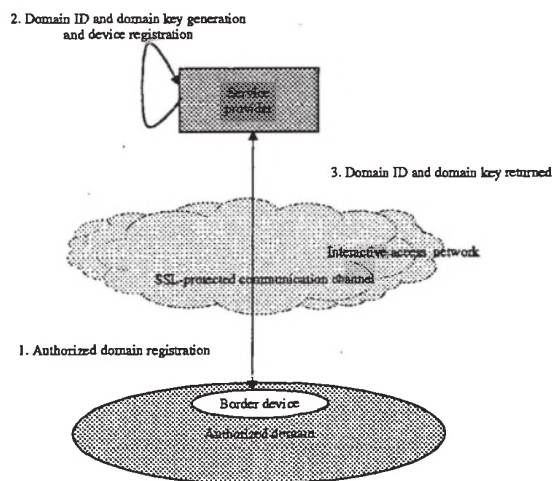


Figure 13: Authorized Domain Registration

A border device is responsible for authorized domain registration because it has a close tie with service provider. The border device may be purchased or rented from the service provider, and contains service provider specific CA module (or DRM terminating module) within the device.

Device public/private key pair and digital certificate obtained by device manufacturer from certificate authority are pre-installed in border device at factory.

The registration procedure can be summarized as follow:

1. Border device establishes a secured and authenticated communication channel with service provider over the interactive access network (e.g. using SSL). Border device sends an authorized domain registration request to service provider, supplying its own device ID, device public key and other relevant information such as subscription account ID
2. Service provider verifies and approves the request by generating a domain ID and domain symmetric key for the border device
3. Service provider returns the domain ID and domain symmetric key to the border device over the secured communication channel. Border device then installs the domain symmetric key into the local tamper-resistant storage

Note that a group of authorized devices may possess more than one domain ID (and domain symmetric key) if there are more than one border device within the authorized domain, and each border device can receive content from a different service provider. On the other hand, a border device may be able to receive content from more than one service provider, and thus needs to support multiple authorized domains.

Digital certificate technology is used to establish secured and authenticated communication channel between device and service provider. Normally, service provider and border device manufacturer apply digital certificates from the same certificate authority, and thus share the same root certificate. In case different certificate authorities are used, some form of peer-to-peer cross-certification arrangement must be made between certificate authorities, so that service provider and border device can authenticate each other's digital certificate. An alternative is to introduce in the value chain the trust management provider, whose role is to offer a homogeneous trust environment for multiple service providers and device manufacturers, by acting as a centralized and trusted certificate authority.

If CPCM-compliant watermarking is implemented, service provider will also supply the public watermark key to border device, along with the domain ID and domain symmetric key.

5.1.2 Authorized Domain Joining

Figure 14 illustrates the typical procedure for a non-border device of an authorized domain to join an authorized domain.

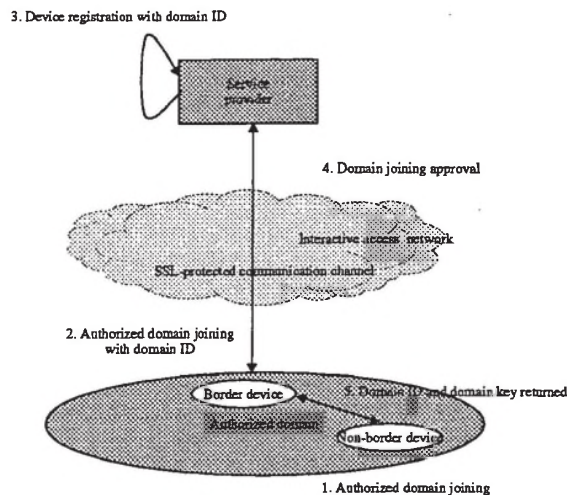


Figure 14: Authorized Domain Joining

Device public/private key pair and digital certificate are pre-installed in non-border device at factory by device manufacturer.

A non-border device can join the authorized domain by executing the following procedure:

1. Non-border device establishes a secured and authenticated communication channel with the border device (e.g. using SSL), and sends an authorized domain joining request to border device
2. Border device determines to accept the request (e.g. by checking user configuration information), and forwards the request with its own domain ID to service provider over another secured and authenticated communication channel over the interactive access network
3. Service provider determines to accept the request (e.g. by checking subscription policy for this particular domain), and registers the non-border device with the domain
4. Service provider sends back the approval to the border device



Proposed Functional Areas

5. Border device sends the domain ID and domain symmetric key to the non-border device, which in turn saves the domain symmetric key into local tamper-resistant storage.

Note that a non-border device may belong to more than one authorized domain. A non-border device can join different authorized domains via border device, which may be associated with different service providers.

The same consideration for digital certificate management in domain registration applies here.

If CPCM-compliant watermarking is implemented, service provider will also supply the public watermark key to non-border device, along with the domain ID and domain symmetric key.

5.1.3 Content Preparation and Distribution

This section describes the mechanism to apply CPCM-compliant watermark to content and potential ways to distribute voucher template to the CPCM system via broadcast network.

5.1.3.1 CPCM-compliant Watermarking

CPCM-compliant watermarking can be performed by content provider. A watermarking unit is used to apply a CPCM-compliant imperceptible watermark to the content. The watermark payload contains the information including content ID (in compressed format) and CPCM version number. The public watermark key used to apply the watermark on the content will be distributed to authorized devices during domain registration and joining. Digital watermarking is an optional feature in the CPCM system.

5.1.3.2 Voucher Template Distribution Mechanisms

The voucher concept allows tremendous flexibility in the way vouchers or voucher templates (untargeted vouchers) can be distributed. There are several methods service provider can choose from depending on the business model.

This proposal foresees the following potential mechanisms to distribute voucher template to CPCM-compliant devices via the broadcast network:

- Delivery as a CPCM-specific descriptor (Mandatory)
- Delivery via CPCM-specific ECM/EMM (Recommended)
- Delivery via CPCM-specific PES (Optional)
- Delivery over IP datacast (Mandatory if IP datacast is supported)
- Delivery from a centralized server via interactive access network (Mandatory alternative)

5.1.3.2.1 Voucher Template Delivery as CPCM-Specific Descriptor

A new CPCM-specific descriptor can be defined for the purpose of carrying voucher templates. This descriptor can be attached to SI tables such as PMT. Attention should be paid to the repetition frequency so that end-users can start making recording at suitable resolution (e.g. 1 ~ 2 seconds). This method is similar to what is used for Copy Control Information in DTCP. The proposed data structure of the CPCM-specific descriptor is as follow:

```
CPCM_descriptor {
    Descriptor_tag                8 uimbsf (value TBD)
    Descriptor_length             8 uimbsf
    For (I=0; I<descriptor_length; I++) {
        CPCM_voucher_byte        8 uimbsf
    }
}
```

5.1.3.2.2 Voucher Template Delivery via CPCM-Specific ECM/EMM

The voucher template data stream is introduced as an additional CA system in the CAT. Voucher templates can be delivered as CPCM ECMs, and related management information through CPCM EMMs. A potential advantage of this method is that, if content keys are delivered in voucher template (as CPCM ECMs) in encrypted form, information required for decrypting them can be delivered in EMMs.

5.1.3.2.3 Voucher Template Delivery via CPCM-Specific PES

At the transport stream level, a certain PID is reserved for the data stream that carries voucher templates. If voucher templates are packed inside PES packets, the advantage is that the presentation time stamp in the PES header can be used to synchronize the voucher templates with the program content. This could be advantageous if it is expected that the usage state of the broadcast content changes frequently.

5.1.3.2.4 Voucher Template Delivery over IP Datacast

Voucher template can be delivered in the file format. The advantage of this method is that IP address can be used to control the destination of voucher template.

5.1.3.2.5 Voucher Template Delivery via Interactive Access Network

Voucher template can be requested from service provider, e.g. via the Internet. This non-broadcast method allows an already targeted voucher to be delivered to the requesting device using the same voucher targeting protocol as in transactions between authorized devices. The downside of this method is that server side may be overloaded if there are a lot of simultaneous requests.

5.1.3.3 Voucher Template Protection during Distribution

The voucher template is protected by digital signature of service provider. The distribution of voucher template in broadcast bitstream may be susceptible to tampering or deletion. To recover from this type of tampering attack, the CPCM-compliant digital watermark can be used. If an authorized device detects the presence of CPCM-compliant watermark but cannot find any recognizable voucher template in broadcast bitstream, then the device can assume that the voucher template has been tampered with, and a default voucher template will be generated with the most restrictive usage state setting (Copy Never and Domain Traversal Disallowed). Since the digital watermark is transparent to legacy device, and can be made very difficult to remove, this provides a backward-compatible and tamper-resistant method to ensure that voucher template delivery over broadcast bitstream is tamper-sensitive and recoverable from tampering attack.

5.2 CPCM-Compliant Operations

The following sections describe how CPCM-compliant operations are performed at high-level.

5.2.1 Content Recording

Figure 15 illustrates a typical configuration for content recording. This is normally the way content enters a CPCM system. Content is delivered over the broadcast network, received by the CPCM-compliant border device (e.g. set-top box) of an authorized domain, and recorded into a CPCM-compliant recording device (e.g. personal video recorder).

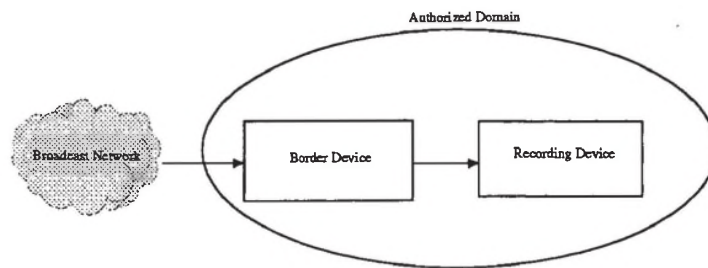


Figure 15: Content Recording

The operation sequence of content recording is as follow:

- Border device terminates native content protection (e.g. CA) of the incoming content
- Border device detects the CPCM-compliant watermark (optional)
- Border device extracts content voucher template from the broadcast bitstream, and checks its data integrity by verifying the digital signature of service provider
- Border device generates a content key using a local key regeneration algorithm (see content key generation mechanism chapter), and uses the content key to encrypt the content

- Border device generates a content voucher with the initial usage state, device-targeted content key and digital signature for the voucher
- Border device retargets the content key using the public key of recording device (and/or domain symmetric key), as described in the copy protection model chapter
- Border device passes the encrypted content and voucher to the recording device
- Recording device checks the data integrity of the incoming voucher by verifying the digital signature of the border device
- Recording device verifies the usage state in voucher
- Recording device saves the encrypted content and voucher in local storage

Exceptions to be handled by the border device include:

- If the incoming content is legacy content, a default voucher with usage state set to "Copy Control Not Asserted and Domain Traversal Allowed" will be associated with the content. The content will not be encrypted.
- If the voucher template is not available in the broadcast bitstream, corrupted or rendered unrecognizable, the border device contacts the service provider for a good voucher template based on content ID
- If the incoming voucher is detected being tampered or the usage state is rendered unrecognizable, the recording device sets the usage state to "Copy Never and Domain Traversal Disallowed". The end-user may use the recording device to contact service provider for voucher renewal or upgrade
- If the recording operation has conflict with the incoming usage state, the recording device may contact the service provider for voucher upgrade.

5.2.2 Content Downloading

Figure 16 illustrates a typical configuration of content downloading. This is another typical way that content enters a CPCM system. Internet content is downloaded via the broadcast network, and received by the CPCM-compliant border device (e.g. residential gateway) of an authorized domain, and saved into a CPCM-compliant storage device (e.g. personal computer).

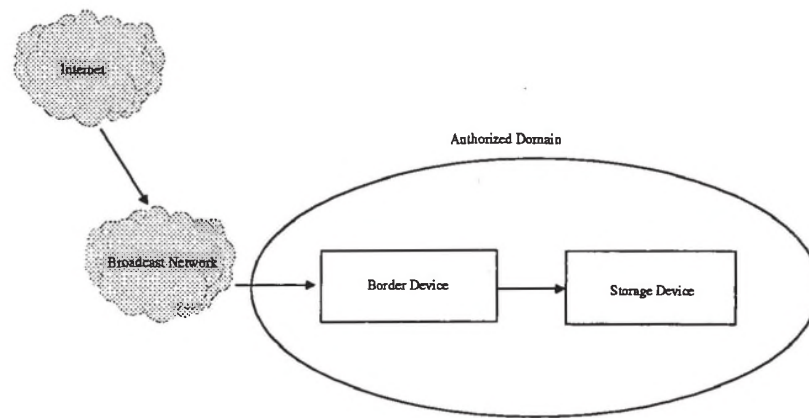


Figure 16: Content Downloading

The operational sequence and exception handling are very similar with that of content recording. One major difference is that the native content protection in this case may be DRM rather than CA.

5.2.3 Content Copying

In general, content copying operation follows the copy protection model specified in previous chapter.

5.2.3.1 Content Copying within Same Domain

Figure 17 illustrates a typical configuration of content copying within same authorized domain. Content and its associated voucher has been stored in one recording device (e.g. personal video recorder), and end-user wants to make a copy in another recording device (e.g. another personal video recorder) within the same domain.

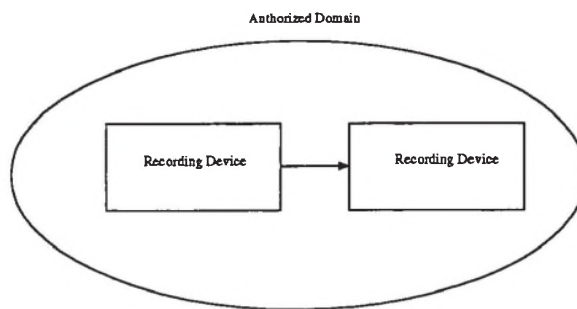


Figure 17: Content Copying within Same Domain

The operation sequence of content copying within the same domain is as follow:

- End-user specifies to source device of the target device and ID of the content to be copied
- Source device sends target device a copy request and gets back the domain ID and public key of the target device, via peer-to-peer protocol over secured communication channel, as described in the copy protection model chapter
- Source device determines that target device belongs to the same domain, and checks the content usage state if there is any conflict with the copy request

- Source device updates the usage state of its own copy of the voucher, and generates a new copy of the voucher with content key retargeted using the target device public key (and/or domain key)
- Source device sends the duplicated copy of the content and voucher to target device
- Target device checks the data integrity of the incoming voucher by verifying the digital signature of the source device
- Target device saves the encrypted content and voucher in its own local storage.

The exceptions to be handled include:

- If the source device determines that the usage state of the content does not permit the copying request, it may fail the copy request, or may need to contact service provider for voucher upgrade
- If the target device detects that the incoming voucher is being tampered or the usage state is rendered unrecognizable, the target device sets the usage state to "Copy Never and Domain Traversal Disallowed". The end-user may need to contact service provider for voucher renewal or upgrade

5.2.3.2 Content Copying across Different Domains

Figure 18 illustrates a typical configuration of content copying across different authorized domains. Content and its associated voucher has been stored in one recording device (e.g. personal video recorder), and the end-user wants to make a copy in another recording device (e.g. another personal video recorder) in different domain.

The operation sequence of content copying across different domains is as follow:

- End-user specifies to source device of the target device and ID of the content to be copied content
- Source device sends target device a copy request and gets back the domain ID and device public key of the target device, via peer-to-peer protocol over secured communication channel, as described in the copy protection model chapter
- Source device determines that target device belongs to a different domain, and checks the content usage state if there is any conflict with the copy request
- If the usage state record specifies that content is allowed to traverse domains, source device updates the usage state of its own copy of the voucher, and generates a new copy of the voucher with content key retargeted using the target device public key, and sends the encrypted content and voucher to target device

- If domain traversal is not allowed and usage state change is allowed, source device forwards the copy request and its own voucher to service provider for further processing. Service provider may request target device to accept a new offer before sending back an updated voucher to source device, and a new voucher to the target device with the appropriate protection
- Target device checks the data integrity of the incoming voucher by verifying the digital signature of source device (or digital signature of service provider if the copying request is handled by service provider)
- Target device saves the encrypted content and voucher in its own local storage.

The exceptions to be handled include:

- If the source device determines that the usage state of the content does not permit the copying request, it may fail the request, or may contact the service provider for voucher upgrade
- If the target device detects that the incoming voucher is being tampered or the usage state is rendered unrecognizable, the target device sets the usage state to "Copy Never and Domain Traversal Disallowed". The end-user may need to contact service provider for voucher renewal or upgrade.

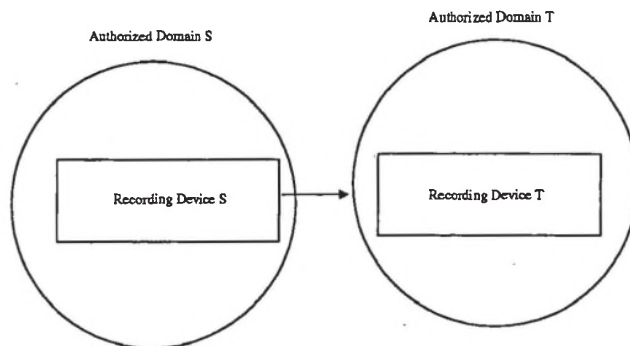


Figure 18: Content Copying across Different Domains

5.2.3.3 Copy Control Not Asserted

If the usage state of content is "Copy control not asserted", the content may be encrypted or not by the border device, depending on the domain traversal flag. If the domain traversal flag is equal to "Allowed", the content is not encrypted and remains in clear form within the CPCM system, and the voucher does not require to hold any content key. On the other hand, if the domain traversal flag is equal to "Disallowed", the content is encrypted and the voucher contains the content key, which is encrypted by domain symmetric key.

The operation sequence of content copying within the same domain is as follow:

- End-user specifies to source device of the target device and ID of the content to be copied
- Source device sends target device a copy request and gets back the domain ID and public key of the target device, via peer-to-peer protocol over the secured communication channel, as described in the copy protection model chapter
- Source device determines that target device belongs to the same domain, and proceeds to check the content usage state if there is any conflict with the copy request
- Source device finds out that the usage state is "Copy control not asserted". Then it checks the domain traversal flag
- If the domain traversal flag is equal to "Allowed", that means the content is not encrypted at all, and there is no content key to protect. Source device proceeds to generate a new copy of the voucher without any content key, and sends it to the target device
- If the domain traversal flag is equal to "Disallowed" that means the content is encrypted by a domain symmetric key. Source device proceeds to generate a new copy of the voucher with content key still encrypted by the same domain symmetric key, and sends it to the target device
- Target device checks the data integrity of the incoming voucher by verifying the digital signature of the source device
- Target device saves the content (encrypted or not) and voucher in its own local storage.

The operation sequence of content copying across different domains is as follow:

- End-user specifies to source device of the target device and ID of the content to be copied
- Source device sends target device a copy request and gets back the domain ID and public key of the target device, via peer-to-peer protocol over the secured communication channel, as described in the copy protection model chapter



Proposed Functional Areas

- Source device determines that target device belongs to different domain, and proceeds to check the content usage state if there is any conflict with the copy request
- Source device finds out that the usage state is "Copy control not asserted". Then it checks the domain traversal flag
- If the domain traversal flag is equal to "Allowed", that means the content is not encrypted at all, and there is no content key to protect. Source device proceeds to generate a new copy of the voucher without any content key, and sends it to the target device
- If the domain traversal flag is equal to "Disallowed" that means the content is encrypted by a domain symmetric key. Source device checks the usage state change flag to see if it is allowed to upgrade voucher. If positive, source device forwards the copy request and its own voucher to service provider for further processing. Service provider may request target device to accept a new offer before sending back an updated voucher to source device, and a new voucher to the target device with appropriate protection. Or the copying request is simply denied by service provider
- Target device checks the data integrity of the incoming voucher by verifying the digital signature of the source device (or digital signature of service provider if the copying request is handled by service provider)
- Target device saves the content (encrypted or not) and voucher in its own local storage.

5.2.4 Content Moving

In general, content moving operation follows the copy protection model specified in previous chapter.

5.2.4.1 Content Moving within Same Domain

Content moving within same domain is very similar to that of content copying within same domain. The only difference is that, in the case of content moving, the original copy of the content and voucher will be erased from the source device.

5.2.4.2 Content Moving across Different Domains

Content moving across different domains is very similar to that of content copying across different domains. The only difference is that, in the case of content moving, the original copy of the content and voucher will be erased from the source device.

5.2.5 Content Rendering

Figure 19 illustrates a typical configuration of content rendering within the same domain. Content may be received by a border device (e.g. set-top box) and forwarded to rendering device (e.g. digital TV). Alternatively, content may have been stored in storage device (e.g. personal video recorder) and playback to rendering device (e.g. digital TV).

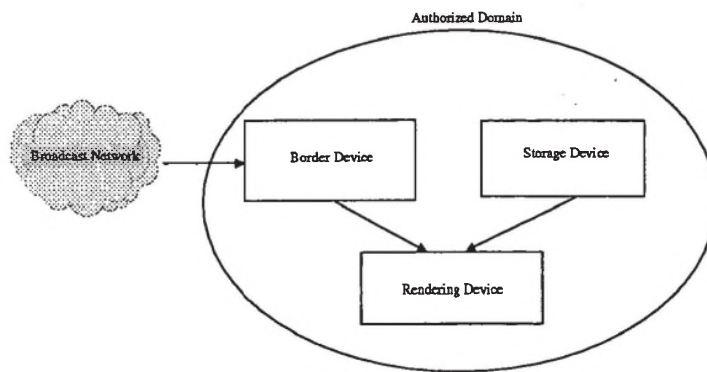


Figure 19: Content Rendering

The operation sequence of content rendering directly from border device is as follow:

- Border device terminates native content protection (e.g. CA) of the incoming content
- Border device detects the CPCM-compliant watermark (optional)
- Border device extracts voucher template from the broadcast bitstream, and checks its data integrity by verifying the digital signature of service provider
- Border device generates a content key using a local key regeneration algorithm to encrypt the content, and uses device public key (and/or domain symmetric key) to encrypt the content key as described in the copy protection model chapter
- Border device generates a voucher with the initial usage state, device-targeted content key and the digital signature for the voucher

- Border device retargets the content key using the public key of rendering device (and/or domain key), which is obtained by secured peer-to-peer communication, as described in the copy protection model chapter
- Border device passes the encrypted content and voucher to the rendering device
- Rendering device checks the data integrity of the incoming voucher from the border device by verifying the digital signature of border device
- Rendering device verifies the usage state in the voucher
- Rendering device decrypts the content and passes it to local decoder and rendering hardware.

The operation sequence of content rendering from storage device is as follow:

- Storage device checks the data integrity of the voucher of the playback content
- Storage device checks and updates the usage state in the voucher to see if there is any conflict in the usage
- Storage device retargets the content key using the public key of rendering device (and/or domain key), which is obtained by secured peer-to-peer communication, as described in the copy protection model chapter
- Storage device passes the content and voucher to the rendering device
- Rendering device checks the data integrity of the incoming voucher, and then extracts the content key using its own device public key (and/or domain key)
- Rendering device decrypts the content and passes it to local decoder and rendering hardware.

5.2.6 Content Backup and Restore

Figure 20 illustrates a typical configuration of content backup and restore. Content has been stored in CPCM-compliant storage device (e.g. personal video recorder), and is to be backup to non-compliant detached storage device (e.g. hard-disk storage).

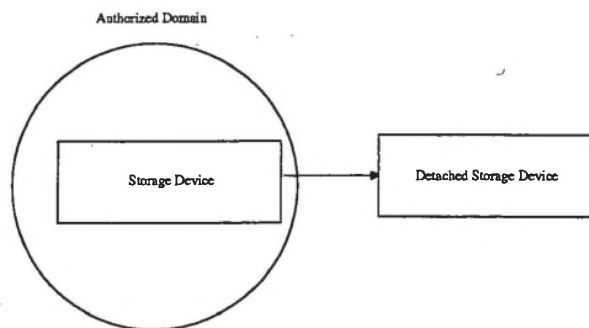


Figure 20: Content Backup and Restore

The non-compliant detached device does not possess any CPCM functionality. The CPCM-compliant storage device simply passes the content and its associated voucher in its present protected format to the backup storage device, and erases the original copy of content and voucher from the source storage. The CPCM-compliant storage device can also restore the backup content and voucher by extracting them from the detached storage device. A check of the data integrity of the voucher will be performed by the CPCM-compliant storage device.

In the worst case where the detached storage device fails, the unlucky end-user may still be able to restore its usage rights from service provider, if the end-user has subscribed some kind of personal locker service.

On the other hand, if a CPCM-compliant storage device dies after backing up its content into a detached storage device, end-user can still restore the content to another target device. The dead device and target device may belong to the same domain or different domains. The content and voucher that was targeted at the dead device are moved to the target device. When the target device attempts to consume (e.g. playback) the content, it tries to contact the dead device and of course fails. The target device then contacts service provider for assisted voucher re-targeting.

5.2.7 Content Superdistribution

Figure 21 illustrates a typical configuration of content superdistribution. An end-user owns a piece of CPCM-compliant content in the recording device (e.g. personal video recorder), and intends to superdistribute the content to another end-user. In this context, superdistribution implies that the distribution or copying of content beyond that the initial usage state allows. The right to consume the content can be purchased separately.

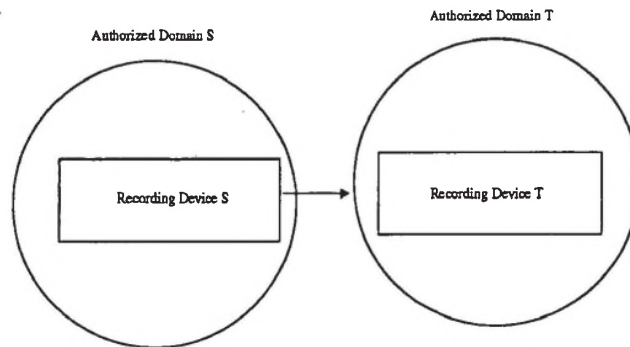


Figure 21: Content Superdistribution

The operation sequence of content superdistribution is as follow:

- Source end-user makes an offer to target end-user via some superdistribution application, e.g. renting, selling
- Target end-user accepts the offer
- Source device forwards the superdistribution request its own voucher to service provider
- Service provider may request target device to confirm the transaction before sending back confirmation to source device, with the new usage state acquired by target device
- Source device decrypts the content key using its own device private key, and then re-encrypts it using target device public key, and generates a new voucher for the target device



Proposed Functional Areas

- Target device checks the data integrity of the incoming voucher by verifying the digital signature of source device
- Target device re-signs the voucher, and saves the content and voucher in its own local storage.

Note that superdistribution may not be conducted in some cases when the usage state change flag is set to "Disallowed".

5.2.8 Content Recording or Downloading First Pay Later

Under this scenario, the CPCM-compliant border device indicates to service provider, via some application interface, that the intention is to record or download the content first and pay later. Another applicable scenario for "Record first, pay later" is that the broadcast service provider may transmit during nighttime some content, in encrypted format, that all receivers can record. This content will be "Tonight's special movie". In order to watch this movie, consumers will need to contact service provider to purchase the usage right separately.

Note that this is in contrary with all the previously covered scenarios, which assume the content has been paid for at (or ahead of) the time of recording and consumption, such that the service provider agrees to target content key to specific authorized devices.

The operation sequence of this feature is very similar to that of content recording or downloading. The major difference is that the border device does not generate any content key during voucher creation. The content is encrypted by service provider at broadcast source using its own content key. The encrypted content and "incomplete" voucher from the border device are stored in the recording device (e.g. personal video recorder).

When the end-user attempts to consume the content (e.g. playback), the consuming device detects that the content key is absent in the voucher, and contacts service provider for help. The service provider then makes an offer to the end-user. Once the offer is accepted, a new voucher with the device targeted content key is returned to the consuming device.

5.2.9 Content Uploading and Rendering in Mobile Devices

Figure 22 illustrates a typical configuration of content uploading and rendering in mobile devices. Content has been stored in CPCM-compliant storage device (e.g. personal computer), and is uploaded to mobile device via USB or infrared connection.

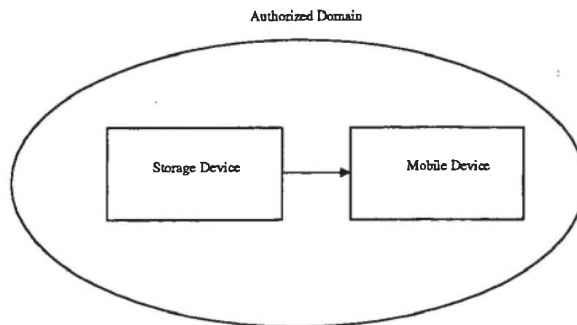


Figure 22: Content Uploading and Rendering in Mobile Device

For high-end mobile devices that possess adequate processing power and storage capacity, this scenario is identical to that of content copying and rendering within same domain.

Low-end mobile devices may lack adequate processing power, storage capacity and cryptographic capability. These mobile devices are considered as non-compliant detached device, and unsafe for CPCM-compliant device to release clear content to these devices directly. A network-side CPCM proxy agent may be required to perform the following:

- The CPCM proxy authenticates low-end mobile devices and ensure that they possess some kind of forward-lock mechanism
- The CPCM proxy is considered as target device for content key encryption
- The CPCM proxy decrypts content on behalf of low-end mobile devices, and deliver the clear content to the mobile devices via secure wireless network.



5.2.10 Content Streaming

Content streaming from one device to one or more other devices is neither copying or moving. It is not copying because the number of persistent copies of content does not increase. It is not moving because the original will not be deleted at the source device.

Under the situation where content is streamed from the Internet through the broadcast network to a streaming client on an authorized domain, the operation sequence is very similar to that described in the previous section "Content rendering directly from border device". In this case, the border device will not keep any copy of the content and voucher, and the voucher targeted at the streaming client device should have a usage state of "Copy never and domain traversal disallowed", to ensure that the streaming client device cannot make any copy of the streaming content.

Under the situation where the content has already been stored in a CPCM-compliant storage device, and another streaming client device intends to consume the content in streaming mode, the operation sequence is very similar to that described in the previous section "Content rendering from storage device". In this case, the voucher targeted at the streaming client device will also have the usage state set to "Copy never and domain traversal disallowed", to ensure that the streaming client device cannot make any copy of the streaming content. However, the voucher usage state in the storage device remains unchanged.

In case of point-to-multipoint streaming, the CPCM system will retarget vouchers for one or more targeting devices based on the aforementioned principles.

5.2.11 Support of Multiple Domains per Device

The proposed CPCM system supports authorized device to register to multiple domains.

If a border device can receive content from more than one service provider, a default domain must be registered for each service provider, to handle exclusively the content from that service provider. Content voucher template contains a field that stores the service provider ID, which can be used to map to the corresponding default domain ID when the voucher template is instantiated into a voucher. Content voucher contains a field that stores the domain ID that the content currently belongs to. This arrangement prevents the adverse scenarios such as the usage right of content from one service provider gets revoked by another service provider.

For non-border devices which have been registered to more than one domains, there is no confusion about which incoming content should belong to which domain, because the content voucher contains the domain ID of the source device.

5.3 Backward Compatibility**5.4 CPCM-compliant Content Entering Legacy System**

Figure 23 illustrates the scenario when CPCM-compliant content enters a legacy border device.

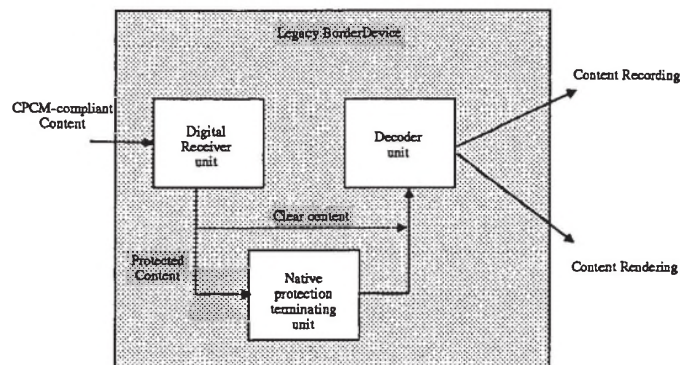


Figure 23: CPCM-Compliant Content Entering Legacy System



The legacy system can process incoming CPCM-compliant content without any problem, because there is no difference between CPCM-compliant content and legacy content in this case. No CPCM encryption will be applied to the content by the legacy border device. The imperceptible watermark embedded in the content will not affect the quality of the content. The voucher template in the broadcast bitstream will be ignored by the legacy system.

5.5 Legacy Content Entering CPCM-compliant System

As described in previous sections, legacy content will be converted into CPCM-compliant format when it enters a CPCM-compliant system the first time, and remains in this format for the remaining life cycle.

6 PROTECTION MECHANISM FOR CONTENT

This section provides a summary of the content protection mechanisms used in this CPCM architecture.

6.1 Proposed Algorithms and Functions*Table 10: Recommended Algorithms*

Item	Description	Remarks
Hashing	SHA-1 NIST Secured Hash Standard	160-bit output
Public key encryption	RSA RFC2437-PKCS#1 RSA Encryption Version 2.0	1024-bit key
Symmetric key encryption	AES NIST Advanced Encryption Standard	128-bit key 128-bit block size
Watermarking (optional)	Proprietary algorithm	

6.2 Content Encryption

Content is protected by symmetric key encryption.

6.3 Content Key Encryption

Content key is targeted to a specific device and/or domain by encrypting it with device public key and/or domain symmetric key, as required by the usage state.

6.4 Voucher Integrity Protection

The data integrity of the voucher, and more importantly, the data integrity of content usage state is protected by digital signature technology.

6.5 Tamper-Resistant Storage

Tamper-resistant storage is required in authorized devices for securing the following items:

- Device private key
- Domain symmetric key

6.6 Digital Watermarking

CPCM-compliant watermark is embedded into content at broadcast source for proof of copyright ownership, and support of CPCM version control. It also serves as a positive distinction of CPCM-compliant content from legacy content and supports a backward-compatible, tamper-resistant method to carry voucher template in broadcast bitstream. Public watermark key is distributed by service provider to authorized border devices during domain registration and joining. Digital watermarking is considered optional in the CPCM architecture.

7 DVB CPCM API**7.1 Baseline CPCM API**

The baseline library may consist of the following modules:

Table 11: Baseline CPCM Library

CPCM Module	DVB CPCM APIs
Cryptographic module	<ul style="list-style-type: none"> • Content encryption/decryption (Symmetric key encryption) • Content key encryption/decryption (Public key encryption) • Content key retrieval • Other security tools (Hashing, Digital Certificate, SSL)
Voucher management module	<ul style="list-style-type: none"> • Voucher updating • Voucher upgrade • Voucher renewal • Voucher copying • Voucher authentication • Voucher retargeting
Service management module	<ul style="list-style-type: none"> • Domain registration • Domain deregistration • Device joining a domain • Device leaving a domain
System management module	<ul style="list-style-type: none"> • System software upgrade • CPCM plug-in management • Tamper-resistant storage management
Application control module	<ul style="list-style-type: none"> • Border control • Recording control

	<ul style="list-style-type: none"> • Rendering control • Playback control • Backup/Restore control
Digital watermarking module (optional)	<ul style="list-style-type: none"> • Watermark detection

7.1.1 Multiple Proprietary Extension Support

Authorized devices can support different proprietary usage state extensions. The interpretation of usage state extensions under some situations are illustrated by Figure 24.

An example of proprietary extension plug-ins interworking is depicted in Figure 25. The operation in this example is to copy a movie from PVR1 to PVR2, where PVR1 has P1 plug-in and PVR2 has P2 plug-in, and the movie has been stored using P1 plug-in extension.

- PVR1 retrieves usage state from the original voucher and recognizes it as "Copy 10 times only". PVR1 approves the copying operation
- PVR2 retrieves content usage state from the retargeted content voucher and does not recognize the usage state extension. Thus, PVR2 interprets the usage state as "Copy never", and disapproves the copying operation.

7.1.1.1 Installation and Authentication of Proprietary Extension Plug-ins

Proprietary CPCM plug-ins can be distributed by service provider and installed on authorized devices. The procedure for ensuring proper authentication of a CPCM plug-in before installation is as follow:

- A digital signature of the CPCM plug-in is generated by using the private authentication key of service provider to encrypt some bios information of the CPCM plug-in (e.g. file name, file size, date, time)
- This digital signature is sent along with the CPCM plug-in to the authorized device
- The baseline CPCM manager of the authorized device verifies the digital signature of the CPCM plug-in using the public authentication key of the service provider
- Once authenticated, the baseline CPCM manager installs the proprietary CPCM plug-in on the authorized device.

It is also recommended that the MHP specification [6] be referenced in the area of installation and authentication of CPCM proprietary extension plug-ins, where applicable.

7.1.1.2 Identification of Proprietary Extension Plug-ins

Content or service provider can define a proprietary extension number to identify the corresponding proprietary extension plug-in. CPCM-compliant authorized devices can select the appropriate proprietary extension plug-in to perform usage state management, by referring to this proprietary extension number. The proprietary extension number can be provider-specific or content-specific. This number can be carried by content voucher template.

7.1.2 Multiple Non-CPCM System Support

The proposed CPCM architecture is agnostic to different content protection systems such as CA and DRM. The native content protection is terminated at the boundary of the CPCM system, and CPCM takes control from there onward. Again, proprietary plug-ins are necessary for mapping right expressions in native content protection system into the corresponding CPCM baseline or extension usage states.

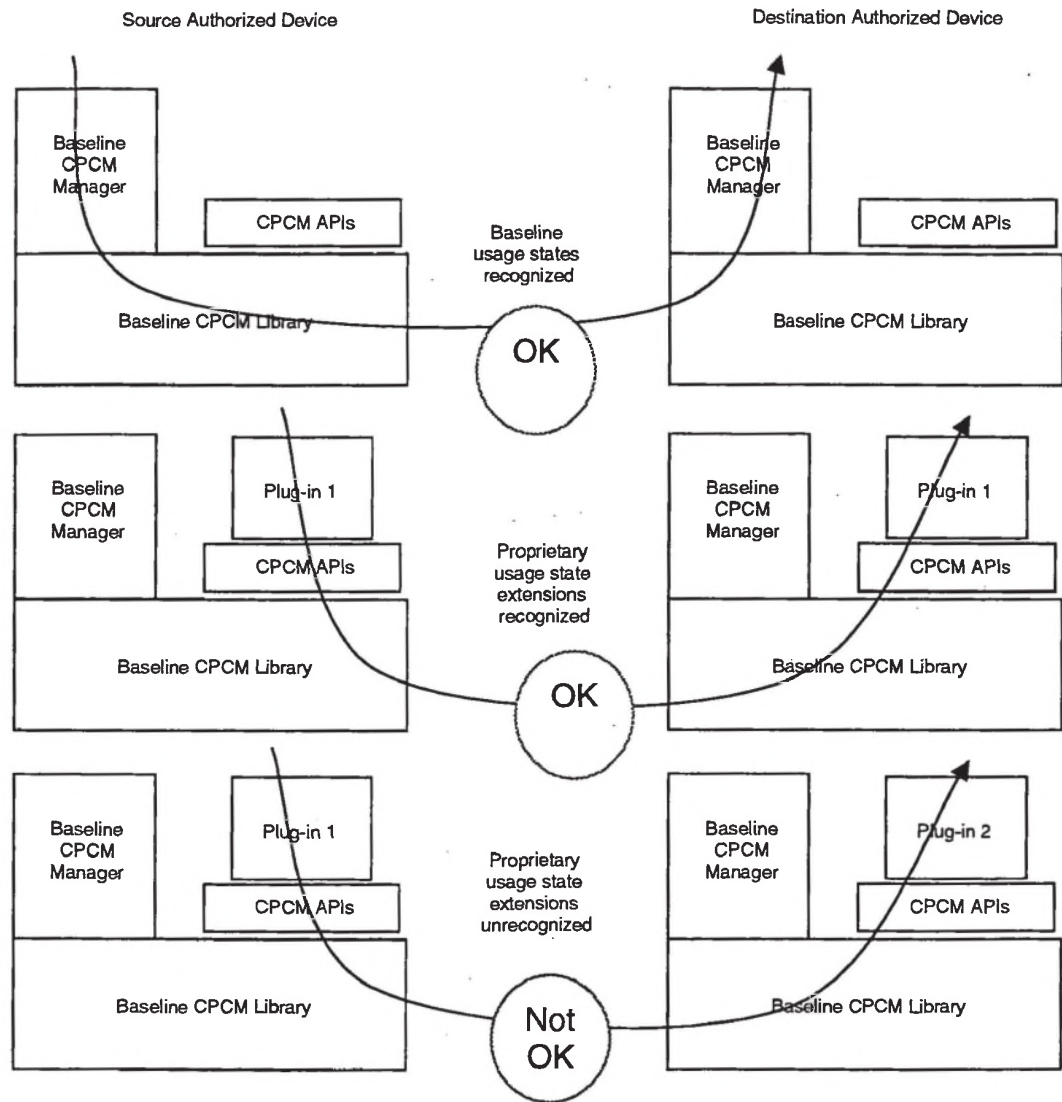


Figure 24: Multiple Proprietary Extension Plug-in Scenarios

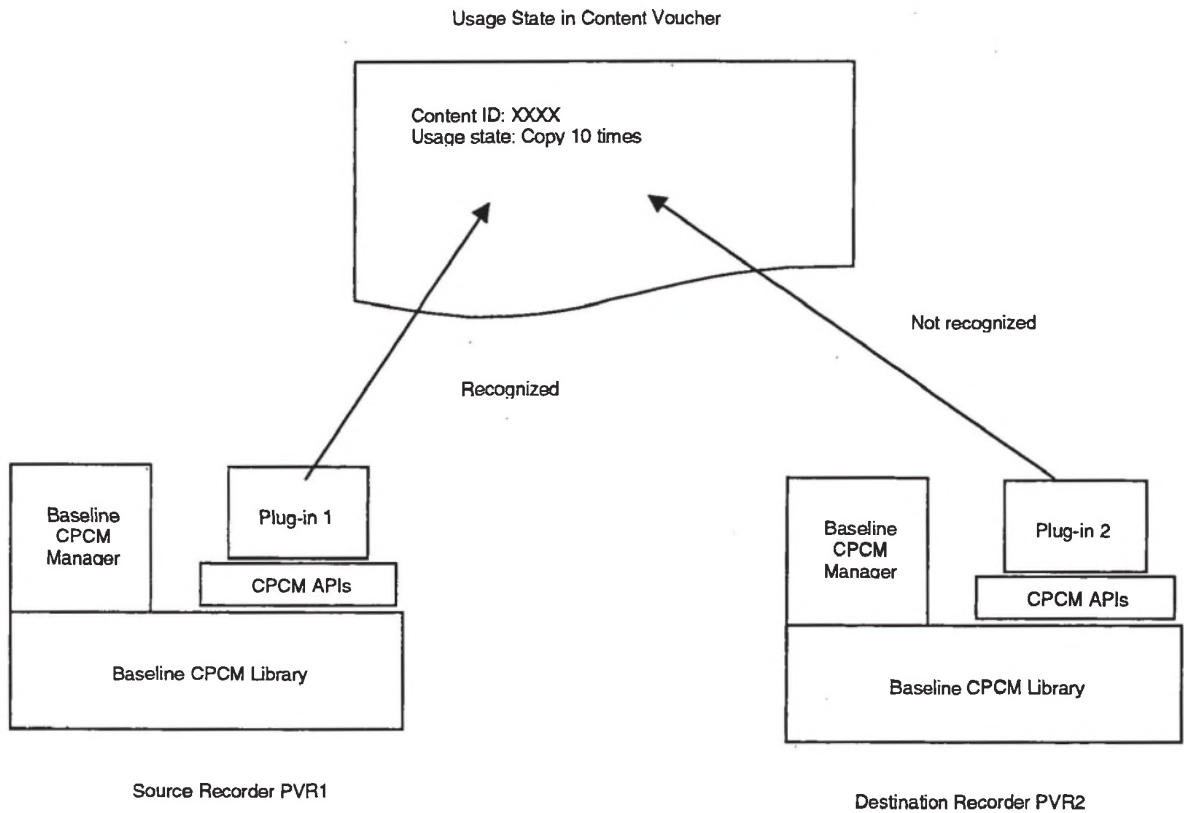


Figure 25: Proprietary Extension Plug-ins Interworking

8 UNDERLYING SECURITY INFRASTRUCTURE

The underlying security infrastructure of the CPCM architecture is summarized as follows:

- Registration of authorized domains and devices are achieved by authentication and authorization services
- Content is protected by native protection mechanism (e.g. CA) in broadcast network and then protected by symmetric encryption when the content enters a CPCM system, and voucher template is carried in broadcast bitstream, and voucher is protected by digital signature technology
- Exchange of content key is secured by device public key encryption and exchange of system messages is secured by SSL-protected channel
- Software upgrade and CPCM plug-ins are secured by digital signature technology.
- Public Key Infrastructure (PKI) is required to support issuance and verification of digital certificates of devices and service provider
- Standard firewall infrastructure is required to protect content and service provider premises.

9 IMPLEMENTATION REQUIREMENTS**9.1 Object Sizes****Table 12: Object Sizes**

Item	Description	Remarks
Baseline usage state	Four (4) baseline options: <ul style="list-style-type: none"> • Copy Control Not Asserted • Copy Once • Copy No More • Copy Never 	2 bits
Usage state record	Usage state + Domain traversal flag + Usage state change flag	8 bits Usage state extension has been considered
Voucher (template)	Voucher (template) ID + CPCM version number + CPCM proprietary extension no. + Content ID + Service provider ID + Initial domain ID + Current domain ID + Usage state record + Content key status + Content key (seed) + Digital signature	554 bits
Watermark payload (optional)	Compressed content ID + Compressed content/service provider ID + CPCM version number	64 bits

9.2 Tamper-Resistant Storage**Table 13: Tamper-Resistant Storage**

Item	Description	Remarks
Device ID	Identification of authorized device	64 bits
Device private key	Private encryption key of device	1024 bits
Domain symmetric key	Symmetric encryption key of domain	128 bits

9.3 Non Tamper-Resistant Storage**Table 14: Non Tamper-Resistant Storage**

Item	Description	Remarks
Device digital certificate	Digital certificate of authorized device	
Device public key	Public key of authorized device	1024 bits
Service provider table	<p>The data structure of the table is as follow:</p> <ul style="list-style-type: none"> • Service provider ID • Service provider public key • Default domain ID assigned to this service provider during domain registration or joining 	
Service revocation list	<p>The data structure of the table is as follow:</p> <ul style="list-style-type: none"> • Domain ID • Device ID 	

9.4 CPCM Baseline Library**Table 15: CPCM Baseline Library**

Item	Description	Implementation Complexity
Cryptographic module	Implements all cryptographic APIs	Standard implementations
Voucher management module	Implements all voucher management APIs	Medium complexity
Service management module	Implements all service management APIs	Low complexity
System management module	Implements all system management APIs	High complexity
Application Control module	Implements all control APIs	Low complexity
Watermarking module (optional)	Implements all watermarking APIs	High complexity

10 USABILITY

All CPCM-compliant devices should be designed to perform simple registration and require minimum human intervention in system set-up.

CPCM-compliant device users are expected to perform the following actions only:

- Establish connectivity to service provider via the interactive access network for domain registration, domain joining, and voucher renewal/upgrade
- Specify device operations as desired: recording, copying, moving, rendering, playback, backup, restore, superdistribution
- Interact with service provider during voucher upgrade or renewal
- In case online content purchase is implemented in a CPCM system, device users may be required to respond to purchase request confirmation.

There is no change in operational procedures for legacy devices to handle CPCM-compliant content.



11 RENEWABILITY, REVOCATION AND RESISTANCE TO OBSOLESCENCE

11.1 Renewability

The CPCM system is designed with the following security renewability in mind to ensure long-term integrity of the system:

11.1.1 System Software Upgrade

Service providers are responsible for delivering system software upgrade to individual authorized devices via the broadcast network.

11.1.2 Domain Renewability

Domain renewability is achieved by supported features including registration and deregistration of authorized domains.

11.2 Revocation

In the CPCM system, the following types of revocation are supported:

11.2.1 Device Revocation

Service provider can maintain a device revocation list. This list can be used to deny all or selective CPCM services to specific authorized devices, including hacked or cloned devices. Service provider can also broadcast device revocation list to disable undesirable authorized devices. When a device is revoked, the domain ID and domain symmetric key will be deleted from device local storage. The device needs to perform domain registration or joining with service provider, if it wants to obtain the CPCM services.

11.2.2 Domain Revocation

Service provider can maintain a domain revocation list. This list can be used to deny all or selective CPCM services to specific authorized domains. Service provider can also broadcast domain revocation list to disable a group of undesirable authorized devices belonging to the same domains. When the group of devices are revoked, the domain ID and domain symmetric key of each device will be deleted from device local storage. The devices need to perform domain registration and/or joining with service provider, if they want to obtain the CPCM services again.

11.3 Resistance to Obsolescence

11.3.1 Scalability

The proposed CPCM architecture is scalable. It can be implemented in a progressive manner, evolving from low to high system complexity. The following advanced features, for example, can be implemented in a later stage:

- CPCM-compliant digital watermark
- Trust management provider
- Content superdistribution and financial/usage clearing.

On the other hand, limited devices such as mobile phones may not have CPCM functionality, but still able to obtain services via CPCM-compliant proxy.

11.3.2 Security Robustness

The proposed CPCM architecture is robust to security breaching:

- Content key is physically separated from the protected content, and is targeted to specific authorized device by encrypting it using device public key and/or domain key. Other devices will not be able to use them, without retargeting by source device or service provider
- CPCM-compliant watermark provides tamper-resistant proof of copyright ownership
- Voucher template in broadcast bitstream is protected by digital signature of service provider
- CPCM device will automatically downgrade the usage right of a piece of content if any voucher tampering is detected.

11.3.3 Foreseeable Circumvention Devices

Hacker or cloned devices will not be able to break into the CPCM system because service provider manages authorized domain registration and joining proactively, and can exclude hacker or cloned devices from participating in the CPCM system, by not releasing domain ID and domain symmetric key.

If tamper-resistant storage is breached and hackers take control of the information including device ID, device private key and domain symmetric key of an authorized device, the damages are limited because:

- Attacker can only take control of contents that he/she has purchased and received via broadcast service providers
- Once detected, broadcast service provider can limit the damage by revoking CPCM services to this kind of broken devices and domains



Renewability, Revocation and Resistance to Obsolescence

- Attacker cannot purchase content using other's account, because each authorized device has its own unique device identification.

Misuse of backups of "Copy once" or "Copy no more" content to restore content to a device from which the original has been moved away after making the backup copy is one potential threat, since moving content within an authorized domain cannot be restricted with the existing baseline usage states. Therefore it is recommended that the backup scheme for such content be based on service provider assistance.



12 SUITABILITY FOR IMPORT OR EXPORT

Devices comprising the proposed CPCM system are likely to meet the criteria set forth by Category 5, Part 2, Note 3 of the Wassenaar Arrangement list of controlled commodities. Therefore it is likely that except for the embargoed destinations (currently Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan) in the national export regulations, there are no restrictions (no export license required) either automatically or after approval by respective national authorities.



13 CURRENT STATE OF DEVELOPMENT

The proposed CPCM system is currently at a conceptual stage, but it relies only on open and widely accepted cryptographic algorithms and techniques to implement. Hence, there should not be much hurdles to overcome in terms of development.



Conformance Statement

14 CONFORMANCE STATEMENT

This section performs a walkthrough of the DVB-CP Summary of Requirements [1] by identifying compliance and non-compliance of the proposed CPCM system with these requirements.

Table 16: Commercial Requirement Walkthrough

Number	Area	Requirement	Compliance/Non-compliance
1	Environment	The DVB CPCM system shall be capable of providing end-to-end protection for content in all processes from the point of initial distribution to the end user through to the point of consumption by the end user.	Complied: End-to-end DVB content protection is achieved by combining native protection and CPCM protection, with secured bridging at CPCM-compliant border devices.
2	Environment	The termination point of the DVB CPCM system shall be the point of viewing/listening by the end user unless the display can output the content in digital form.	Complied: All DVB contents are converted into CPCM-compliant format once admitted into a CPCM system, and remains in this format for the remaining of the life cycle of the content.
3	Environment	The DVB CPCM system shall be applicable to the widest possible range of equipment (and not just restricted to DVB-specific systems or sub-systems).	Complied: The proposed CPCM system is applicable to equipment like DVD player, mobile devices, as well as DRM system.
4	Environment	The DVB CPCM system shall be independent of the delivery mechanisms (i.e. transport media/protocols): e.g. the system should be applicable to content received via the cable, terrestrial and satellite systems, the Internet or pre-recorded media.	Complied: The proposed CPCM system is applicable to content received via DVB-C, DVB-T, DVB-S and pre-recorded media like DVD, and Internet media.
5	Environment	The DVB CPCM system shall interact with other CPCM systems in a manner such that the rights delivered with the content are preserved.	Complied: This is achieved by proprietary CPCM plug-ins.
6	Environment	The DVB CPCM system shall function with or without a CA system whose function is to deliver protected content to the consumer.	Complied: The proposed CPCM system can handle both clear and native-protected content at CPCM-compliant border devices.
7	Environment	The DVB CPCM system shall not rely on the availability of a live return data channel to the content/service provider but may rely upon it if a service provider chooses to operate their domain in this way.	Complied: The proposed CPCM system does not rely on the availability of a live return data channel in the broadcast network. However, vouchers or voucher upgrades may also be requested from service provider through interactive access network if the service provider chooses to operate the service in that way.
8	Functionality	The DVB CPCM system shall be capable of protecting all DVB stream-types, including subtitling, teletext, object and	Complied: The proposed CPCM system does not



Conformance Statement

		data carousels and private data. The priority is to protect the primary picture and sound of television services.	differentiate different DVB stream-types when providing services.
9	Framework	The specified DVB CPCM baseline system shall be able to provide content providers with the necessary protection for their content.	Complied: All DVB contents are converted into CPCM-compliant format once admitted into a CPCM system, and remains in this format for the remaining of the life cycle of the content. The baseline usage state is used to control the content protection and copy management.
10	Framework	The authorized copying, moving and consumption (Authorized usage) of content protected by the baseline DVB CPCM system shall be described by usage state information which shall be tightly bound to the content.	Complied: A content voucher, which contains the usage state and encrypted content key, is created and bound logically to the content, and the binding remains effective for the entire life cycle of the content.
11	Framework	The DVB CPCM system shall include a generic framework, which supports a plurality of proprietary CPCM plug-ins, which can be used by any device conforming to the DVB CPCM specification.	Complied: CPCM APIs are defined to support development of proprietary CPCM plug-ins, to be installed in a CPCM system. The CPCM APIs support extension of usage state beyond the baseline definition. The CPCM proprietary extension number in the content voucher provides the hook for the CPCM system to manage proprietary CPCM plug-ins.
12	Framework	There shall be a DVB specified interface between the CPCM generic system and the proprietary plug-ins.	Complied: CPCM APIs are defined to support development of proprietary CPCM plug-ins, to be installed in a CPCM system. The CPCM APIs support extension of usage state beyond the baseline definition. The CPCM proprietary extension number in the content voucher provides the hook for the CPCM system to manage proprietary CPCM plug-ins.
13	Functionality	<p>The baseline DVB CPCM system shall support the following usage states: Copy control not asserted, Copy once, Copy no more, Copy never. A secure mechanism shall be provided whereby an authorized and authenticated agent may change, subsequent to delivery, the usage state associated with an item of content from any usage state to any other usage state unless the content is marked "Change of usage state is not permitted".</p> <p>The baseline system DVB CPCM system shall also support a means of indicating whether protected content may be moved for consumption outside the Authorized Domain. Rights owners may use a usage state extension to specify additional rules for the authorized usage of the content. The content of such usage state extensions may be proprietary (i.e. not specified by the DVB) and shall be capable of being decoded only by the appropriate proprietary plug-in connected</p>	<p>Complied:</p> <p>A content voucher is created and bound logically to DVB content. The content voucher contains the usage state information of the content, which is allowed to be updated whenever there is a legitimate operation on the content.</p> <p>A usage state change flag is introduced in the content voucher to limit any change of usage state. A domain traversal flag is also introduced in the content voucher to limit any transfer of content across authorized domains.</p> <p>Usage state extensions are handled by introduction of proprietary CPCM plug-ins, which supports mapping of usage state extensions among different proprietary CPCM systems.</p> <p>If there is a mismatch of proprietary plug-ins, the unrecognized usage state is</p>



Conformance Statement

		to the DVB baseline CPCM via the DVB standardized interface. Devices which do not have the appropriate plug-in fitted shall interpret content with any such usage state extensions as "Copy never" and shall respond accordingly. N.B. Proprietary plug-ins shall not require capabilities or resources in the baseline DVB CPCM system beyond those needed to implement the baseline DVB CPCM system.	mapped to "Copy never".
14	Framework	It shall be possible for a device to pass control of: (a) content; (b) CPCM to another qualifying CPCM device provided that the same has an appropriate interface with the DVB CPCM system.	Complied: CPCM control can be passed in the form of usage state inside content voucher among devices. Content control can be passed to other devices by passing content key within content voucher.
15	Framework	The DVB CPCM system shall not allow one proprietary CPCM plug-ins to circumvent or modify another one.	Not addressed by this proposal.
16	Framework	The baseline DVB CPCM system shall not be subverted by proprietary CPCM system.	Not addressed by this proposal.
17	Framework/Security	Access to the DVB CPCM by plug-ins shall be subject to authentication of each plug-in.	Complied: Each plug-in has its own digital signature such that the CPCM system can authenticate the plug-in as trusted application.
18	Framework	The requirements that a downloadable proprietary CPCM plug-in has of the target device (e.g. memory space) must be specified.	Not addressed by this proposal.
19	Framework	The DVB CPCM system shall support the definition and use of "domains" and the application of usage states associated with each item of content to control movement and copying within and across domain boundaries. A mechanism is required for securely defining and implementing "Authorized Domains".	Complied: An authorized domain is created when a border device registers itself with a service provider. A domain ID and domain symmetric key are issued to the registered border device. Similarly, non-border devices receive domain ID and domain symmetric key by performing domain joining via border device within the domain.
20	Framework	DVB CPCM compliant devices, including those, which do not use on-line authentication, shall be capable of being denied specific content in accordance with a revocation list.	Complied: The service provider maintains device and domain revocation lists. It can deny requested CPCM services for specific content to revoked device or domain. It can also terminate CPCM capability of authorized devices by proactively erasing domain ID and domain symmetric key of revoked devices.
21	Functionality	The DVB CPCM system shall enforce limitations of use and copying of the content in accordance with the usage states information conveyed with the content.	Complied: The CPCM system enforces the usage state within the voucher associated with a piece of content.



Conformance Statement

22	Functionality	The DVB CPCM system shall provide a means whereby the rights-protection state and associated usage rules of each item of content can be signaled to each viewer clearly and unambiguously both before and after recording.	Complied: Usage state is stored inside content voucher, which is passed along with encrypted content. Content cannot be consumed unless a valid content voucher is accompanying the content.
23	Functionality	The DVB CPCM system shall allow recording of transmissions or downloads of "Copy once" content. When a copy is made of this content, original download will either be deleted or made inaccessible and the copy of the content will be remarked "Copy no more" such that the copy is protected in a manner to prevent further copying. N.B. For the avoidance of any doubt, the requirement to modify the usage state "Copy once" or "Copy no more" applies only to devices which are capable of creating copies and not to devices which can only playback and/or display the content.	Complied.
24	Functionality	The DVB CPCM system shall allow "Copy no more" content to be moved from one storage device to another (but not copied) (e.g. Moving a piece of music from a hard disc store to a portable memory module for on-the-move listening) provided that such a device is in the same Authorized Domain.	Complied.
25	Functionality	The DVB CPCM system shall not debar the presentation of information to the end user about the extent of copying and serial copying that is allowed for each programme or content object making up such a programme.	Complied: The usage state in content voucher is not encrypted but protected by signed hash.
26	Functionality	The DVB CPCM system must provide protection of content (such that, to the extent possible, only the use authorized by the usage states information is permitted) flowing across/between both analogue and digital interfaces/interconnections/devices within the Authorized Domain.	Complied: All analogue and non CPCM-compliant devices are handled as legacy devices, based on the backward compatibility principle of the proposed CPCM system.
27	Functionality	The DVB CPCM system shall support all known forms of scheduling and payment systems including VoD and be flexible enough to allow new business models to be developed.	Complied: The separation of content and voucher (usage state) allows great flexibility in implementing new business models.
28	Functionality	The functionality of the DVB CPCM system shall be scalable to reflect the capabilities of the connected devices e.g. devices without persistent storage capability shall have simpler CPCM functionality.	Complied: The proposed CPCM system is scalable and can be implemented from low system complexity to high system complexity, e.g. digital watermarking is high complexity. In addition, for limited devices such as home entertainment/mobile devices, CPCM proxy is recommended to assist these limited devices in CPCM operations.
29	Functionality	The renewable security elements of the DVB CPCM system shall all be capable of being renewed at an economic cost throughout the lifetime of the relevant CE	Complied: The renewability service is provided by service provider via interactive access



Conformance Statement

		equipment.	network and/or broadcast network.
30	Functionality	Usage rules for proprietary plug-in modules to the DVB CPCM systems may be conveyed by downloadable data/applications. The DVB CPCM system shall support the conveyance of private/proprietary data to proprietary plug-in modules.	TBD.
31	Functionality	The DVB CPCM system shall allow the user to move content that they have an entitlement to view/store from one storage medium to another for the purpose of replacing or upgrading equipment.	Complied.
32	Functionality	Any watermarks embedded in the content will be passed through the end-to-end DVB system in the same manner as content. No special consideration will be given to the handling or processing of embedded watermarks by the DVB CPCM (except for any watermarking defined as a component of the DVB CPCM system by CPT). It will be the responsibility of the non DVB CPCM watermark technology provider/user to ensure that their watermarks are robust enough to pass through the DVB CPCM system.	Complied.
33	Performance measures	The DVB CPCM system shall not introduce any perceptible degradation of content quality as perceived by the majority of end users (Requirement to be quantified by DVB CPT Technical Group).	Complied: Content is protected by standard encryption technology, and original content quality is preserved after decryption.
34	Performance measures	The DVB CPCM system shall not introduce unacceptable delays in delivery of content as perceived by the majority of end users nor any impairment to the synchronization of picture, sound and data services (Requirement to be quantified by DVB CPT Technical Group).	TBD.
35	Robustness	The transmission of the DVB CPCM usage states information must be as robust as that of the content, which it protects.	Complied: Content voucher is protected by digital signature technology. The usage state inside content voucher can be in clear form or protected by encryption.
36	Robustness	The transmission of the usage states information must survive transcoding of the transport streams to a lower bit-rate and other normal digital distribution processes.	Complied: Initial usage state is transmitted within voucher template, which is distributed from broadcaster to authorized devices via various robust delivery methods: <ul style="list-style-type: none"> • CPCM-specific descriptor • CPCM-specific ECM/EMM • CPCM-specific PES • IP datacast • Interactive access network.



Conformance Statement

37	Security	The DVB CPCM system should be designed such that the requirement for making devices tamper-proof and tamper-evident is minimized and localized to those elements (e.g. secure chips) which hold cryptographic secrets and not extended to requiring physical security of the whole device. It is, nevertheless, acknowledged that in implementing the DVB CPCM system making device tamper-proof and tamper-evident would be an important contribution towards security.	Complied: Tamper-proof requirement is minimized to secured storage of device private key, domain symmetric key.
38	Security	Management of cryptographic secrets (if any) in the DVB CPCM system shall not require that a single overall centralized licensing authority is established and used.	Complied: PKI is required to support digital certificate verification of devices and service provider. Cross-certification arrangement between certificate authorities can relieve the requirement of a single overall centralized licensing authority.
39	Security	Management of cryptographic secrets (if any) in the overall DVB CPCM system may require the use of device revocation in instances of cloned, stolen or lost device keys but such device revocation shall be in respect of a particular service or group of services and shall not inhibit the operation of the device entirely.	Complied: The service provider maintains device and domain revocation lists.
40	Security	If content does not include recognizable DVB CPCM information the appropriate usage rule shall be deemed to be "Copy control not asserted".	Complied.
41	Security	If the DVB CPCM information associated with an item of content is found to be corrupted or unintelligible due to errors (but still recognizable as DVB CPCM information) the appropriate usage rule shall be deemed to be "Copy never".	Complied.
42	Compatibility	The DVB CPCM shall be backwards compatible with legacy devices to the extent possible without compromising functionality or security or adding significant to the cost.	Complied: Usage state is carried by CPCM-specific broadcast bitstream separated from DVB content stream. Legacy system can pick up clear content stream after hand-off by CA module.
43	Inter-device interfaces	The DVB CPCM specification must define a standardized external digital interface between DVB CPCM compliant devices such that: (a) protected content; (b) usage states information; and (c) control of content usage can be securely exchanged between two or more DVB CPCM devices. A means must be provided to establish trust prior to secure exchanges between CPCM compliant devices.	Complied: SSL is applied to establish secured communication channel between authorized devices for peer-to-peer protocol exchange. Content is in encrypted format in transit and does not require extra protection. Public information such as device public key and domain ID may be exchanged over SSL channel.
44	N/A	N/A	N/A
45	Levels and profiles of DVB-CPCM baseline system	The DVB CPCM baseline system shall initially comprise a single profile and level. However, to the extent possible without adding significantly to cost and/or delay in implementation, consideration should be given to facilitating the future provision of	TBD.

NOKIA

Conformance Statement

		additional levels and profiles to the DVB CPCM system in a way which is backwards compatible with the original single profile and level.	
--	--	--	--